vbw

Die bayerische Wirtschaft




Studie

Datenschutz, IT-Sicherheit und Haftung bei automatisierten Systemen

Eine vbw Studie, erstellt vom Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht, Universität Passau

Stand: Juli 2017

Vorwort

Das Recht als Enabler für automatisierte Systeme

Automatisierung ist heute schon aus Wirtschaftsleben und Alltag der Menschen nicht mehr wegzudenken. Die Einsatzbereiche sind vielfältig und reichen vom Industrieroboter über vielfältige Assistenzfunktionen im Kfz oder den Autopiloten im Verkehrsflugzeug bis hin zu Apps auf dem Smartphone. Es zeichnet sich deutlich ab, dass sich der Trend parallel zu den Fortschritten bei der Künstlichen Intelligenz – Stichwort Maschinelles Lernen – weiter fortsetzen und beschleunigen wird.

Der Zukunftsrat der Bayerischen Wirtschaft hat schon im Jahr 2015 betont, wie wichtig es für den Standort Bayern ist, innovationsfreundliche Regelungen für den Einsatz automatisierter Systeme zu schaffen, um möglichst viel Wertschöpfung in Bayern und Deutschland zu generieren. Im Hinblick auf das automatisierte Fahren beispielsweise wurden zwischenzeitlich seitens des Gesetzgebers erste Schritte für eine Erleichterung des Einsatzes unternommen, denen noch weitere folgen müssen.

Teilweise werden auch Rufe laut, möglichen neuen Risiken ebenfalls gleich mit gesetzlichen Regelungen zu begegnen. Aktionismus ist hier aber fehl am Platz: Es muss vielmehr immer zunächst geklärt werden, inwieweit das geltende Recht bereits im Stande ist, das technisch Mögliche und seine Folgen zutreffend abzubilden. Dies unternimmt nun die vorliegende Studie unter dem Blickwinkel von Datenschutz, Datensicherheit und Haftungsfragen bei automatisierten Systemen, mit einem Fokus auf intelligente Objekte wie beispielsweise Roboter oder Drohnen. Sie baut damit auf den Positionspapieren der vbw – Vereinigung der Bayerischen Wirtschaft e.V. zum automatisierten Fahren auf und erweitert den Blickwinkel auf andere Anwendungsfelder.

Im Ergebnis bestätigt die Studie, was der Zukunftsrat in seinen Handlungsempfehlungen von 2017 formuliert: spezielle „Robotergesetze“ sind gegenwärtig nicht erforderlich und deshalb auch nicht zu empfehlen. Regelungsbedarf besteht lediglich punktuell, etwa bei der Frage der Haftung des Netzbetreibers für Störungen und Unterbrechungen, oder bei bestimmten Fragen des IT-Sicherheitsrechts.

Die in den neuen Technologien liegenden Chancen sind groß, die Risiken aber nach bisherigem Stand beherrschbar. In vielen Bereichen bergen die Neuentwicklungen sogar das Potenzial, eine Gefährdung für Menschen und Sachen im Vergleich zum Status Quo zu verringern. Es gilt in jedem Fall weiterhin, die technologische Entwicklung positiv zu begleiten und die Rechtsanwendung aufmerksam zu beobachten, um etwaigen Handlungsbedarf frühzeitig zu erkennen.

Bertram Brossardt
12. Juli 2017

Inhalt

1 Einführung

Begriffsbestimmungen, Status Quo und weitere Entwicklungsschritte

Automatisierte Systeme sind aus unserem Alltag schon heute nicht mehr wegzudenken. So sind etwa unsere Autos bereits imstande, hochautomatisierte Fahrfunktionen auszuführen und auch automatisierte Lieferdrohnen befinden sich bereits in der Test- und Erprobungsphase. Doch auch unser Zuhause wird mit dem Einsatz intelligenter Haushaltsgegenstände zunehmend „smart“ und automatisiert. Zukünftig werden wir insbesondere auch im privaten Bereich sowie im Dienstleistungssektor vermehrt intelligente und automatisierte Systeme antreffen, die uns etwa in Geschäften beraten oder uns im Haushalt aushelfen können.

Die Kehrseite dieser Automatisierung sind jedoch neuartige Gefährdungen, denen durch eine rechtskonforme und sichere Technikgestaltung entgegengewirkt werden muss. Dies betrifft zum einen die Gewährleistung von Funktions- und Informationssicherheit. Zum anderen ist bei der Entwicklung von automatisierten Systemen stets das geltende Datenschutzrecht zu beachten. Wird durch ein automatisiertes System eine Person verletzt oder eine fremde Sache beschädigt, stellt sich weiterhin auch hierbei stets die Haftungsfrage, die durch den Einsatz von automatisierten Systemen eine neue Dimension erhält.

Diese juristische Studie widmet sich der IT-sicherheitsrechtlichen, datenschutzrechtlichen und haftungsrechtlichen Perspektive des Einsatzes automatisierter Systeme. Behandelt werden nicht nur automatisierte Straßen- und Luftfahrzeuge, sondern darüber hinaus auch automatisierte Industrie- und Dienstleistungsroboter und mithin eine Vielzahl verschiedener automatisierter Systeme.

1.1 Begriffsbestimmungen

Im Rahmen der Automatisierung und Smartifizierung werden verschiedene Begrifflichkeiten verwendet, die zunächst definiert werden müssen.

1.1.1 Automatisierung

Der Begriff der Automatisierung wird in der Praxis uneinheitlich verwendet. Zunächst wird hierunter klassischerweise die Übertragung einzelner Aufgaben vom Menschen auf einzelne künstliche Systeme (bspw. auf einen Industrieroboter) verstanden. Aufgaben, die ursprünglich von einem Menschen durchgeführt werden mussten (bspw. Lackierung einer Karosserie) oder für die bislang zumindest eine menschliche Steuerung einer Maschine notwendig war, können von dem automatisierten System (bspw. Lackierroboter oder automatisierte Lackierstation) nun eigenständig und ohne fremde

Hilfe erledigt werden. Dieser Automatisierungsbegriff muss je nach Automatisierungsgrad weiter unterteilt werden. Häufig anzutreffende Begrifflichkeiten sind dabei etwa die Teilautomatisierung, die Hochautomatisierung oder die Vollautomatisierung (vgl. hierzu noch Kapitel 1.2). Daneben existiert als Vorstufe noch das sog. Assistenzsystem und als höchste Form der Automatisierung die sog. Autonomie.

Neben diesem komponentenbezogenen Verständnis von Automatisierung, das den Grad an Verselbstständigung einzelner IT-Systeme / -Komponenten oder Maschinerie beschreibt (bspw.: ein Lackierroboter / ein automatisiertes Fahrzeug), wird auch im Kontext der sog. „Industrie 4.0“ häufig insoweit von einer Automatisierung gesprochen, als durch die Industrie 4.0 sog. „Smart Factories“ ermöglicht werden, in denen gesamte Produktionszyklen automatisiert ablaufen können. Die Industrie 4.0 stellt jedoch keine vertikale Erweiterung der Automatisierungsstufen (über die Stufe der Autonomie hinaus), sondern vielmehr eine horizontale Vernetzung der automatisierten Einzelsysteme, dar.

1.1.2 Autonomie

Autonomie stellt die höchste Stufe der Automatisierung dar und beschreibt je nach Art und Typ des Systems eine vollständige Kontrollübernahme durch die künstliche Intelligenz des Systems. Ein autonomes System bedarf insofern in keiner Situation einer menschlichen Steuerung mehr. Bei einem autonomen Fahrzeug etwa ist ein Fahrzeugführer als solcher daher nicht mehr notwendig. Jeder Insasse des Fahrzeugs wird zum Passagier.

1.1.3 Künstliche Intelligenz sowie Machine Learning

Künstliche Intelligenz (auch: artifizielle Intelligenz) beschreibt die Automatisierung intelligenten Verhaltens; hierzu zählt bspw. die Fähigkeit eines IT-Systems, aus rohen Sensordaten sinnvolle Informationen zu gewinnen und hierdurch selbstständig Rückschlüsse zu ziehen, die dann Auswirkung auf die weitere Programmausführung haben. Künstliche Intelligenz kann von einem IT-System etwa genutzt werden, um aus mehreren möglichen Handlungsalternativen die geeignetste und sinnvollste Option selbstständig auszuwählen (bspw.: Berechnung der optimalen Ausweichroute bei der Erkennung eines Hindernisses durch eine Flugdrohne). Ein Teilbereich der künstlichen Intelligenz ist dabei das sog. „Machine Learning“, bei der das IT-System per Produkteigenbeobachtung oder per „trial-and-error“-Verfahren die in einer spezifischen Situation geeignetste Handlungsalternative für die Zukunft erlernen kann. Durch die zusätzliche Vernetzung der einzelnen selbstlernenden IT-Systeme kann zudem eine sog. „Schwarmintelligenz“ gebildet werden.

Der Einsatz von künstlicher Intelligenz ist auf jeder Automatisierungsstufe möglich. Mit zunehmendem Automatisierungsgrad steigt dabei die Notwendigkeit des Einsatzes höher entwickelter Formen von künstlicher Intelligenz.

1.2 Entwicklung einer allgemeinen Abstufungslehre für automatisierte Systeme

Es wurde bereits gezeigt, dass der Automatisierungsbegriff eine weitere Unterteilung je nach Ausprägung und Grad der Automatisierung erfahren muss. Hinsichtlich automatisierter und autonomer Straßenfahrzeuge existiert hierzu eine Stufenlehre, die den Automatisierungsgrad in fünf Stufen unterteilt,[1] wobei mit steigendem Automatisierungsgrad eine zunehmende Steuerungsübernahme durch das System (technisches Können) und mithin die Möglichkeit des Fahrzeugführers, die eigene Fahrzeugkontrolle abzugeben (rechtliches Dürfen), verbunden ist. Die auf einer spezifischen Automatisierungsstufe von dem System nicht übernommenen Steuerungsarten verbleiben dagegen bei dem Fahrzeugführer, die dieser insofern weiterhin aktiv auszuführen und zu kontrollieren hat. Die verschiedenen Automatisierungsstufen sind dabei die *Assistenz*, die *Teilautomatisierung*, die *Hochautomatisierung*, die *Vollautomatisierung* und die *Autonomie*. Diese Stufenlehre war auch bereits Gegenstand des vbw Positionspapiers „Zukunft automatisiertes Fahren: Rechtliche Hürden beseitigen“ v. Dezember 2015 (S. 4 f.):

Abbildung 1
Stufen des automatisierten Fahrens

* spezifischer Anwendungsfall je nach Straßentyp, Geschwindigkeitsbereich oder Umfeldbedingungen

Quelle: bayme vbm vbw

Fraglich ist, ob diese Kfz-spezifischen Automatisierungsstufen nun allgemein auf alle automatisierten IT-Systeme übertragen werden können. Geht es bei der Automatisierung im Kfz stets um ein automatisiertes Fahren im Straßenverkehr, kann der Einsatzzweck anderer automatisierter Systeme aber auch in der Erledigung anderer Aufgaben

[1] Dagegen enthält die DIN-Norm 19233 etwa lediglich eine Unterscheidung der Stufen „Vollautomatisierung“ und „Teilautomatisierung“.

liegen. Um obige Abstufungslehre daher auf alle automatisierten Systeme anwenden zu können, ist insofern eine Abstraktion dieses Schemas notwendig. Diese könnte folgendermaßen formuliert werden:

– *Stufe 1 (assistiert)*: Das System ist imstande, den Menschen bei der Durchführung seiner Aufgabe zu unterstützen. Das System ist jedoch nicht imstande, die gesamte Aufgabe selbstständig auszuführen, sondern nimmt dem Menschen lediglich eine Teilaufgabe ab. Das assistierte System ist stets von einer zusätzlichen menschlichen Steuerung und Führung abhängig.
Beispiel: Sog. „Exoskelett" zur Unterstützung bei Trag- und Hebearbeiten im Gewerbe oder zur Anwendung bei querschnittsgelähmten Menschen.
– *Stufe 2 (teilautomatisiert):* Das System ist imstande, in *spezifischen* Situationen die zugewiesene Aufgabe selbstständig zu übernehmen. Das System muss dabei aber durchgehend überwacht werden. Notfalls muss von der beaufsichtigenden Person unverzüglich eingegriffen werden.
Beispiel: Einsatz einfacher Fließbänder in der Industrie ohne eigene Fehlererkennungsmechanismen.
– *Stufe 3 (hochautomatisiert):* Das System ist imstande, in *spezifischen* Situationen die zugewiesene Aufgabe selbstständig zu übernehmen. Das System muss nicht durchgehend überwacht werden. Im Bedarfsfall, wenn das System ein Problem erkennt oder ein Fehler auftritt, kann eine menschliche Steuerungsübernahme oder ein regulierender Eingriff notwendig werden. Der Eingriff muss nicht unverzüglich, aber alsbald erfolgen. Das System geht zwischenzeitlich in einen Wartezustand über.
Beispiel: Einsatz fortgeschrittener Fließbänder in der Industrie mit zahlreichen Sensoren und Fehlererkennungsmechanismen, jedoch ohne eigene Fehlerbeseitigungsmechanismen.
– *Stufe 4 (vollautomatisiert):* Das System ist imstande, in *spezifischen* Situationen die zugewiesene Aufgabe selbstständig zu übernehmen. Das System muss nicht überwacht werden. Ein menschlicher Eingriff ist im Rahmen der Leistungsgrenzen auch beim Vorliegen eines erkannten Problems oder eines Fehlers nicht mehr notwendig, da das System imstande ist, dieses selbstständig zu umgehen oder zu beseitigen.
Beispiel: Einsatz hochentwickelter Fließbandsysteme in der Industrie, die mittels zahlreicher Sensorik und intelligenter Fehlererkennungsmechanismen abnormale Zustände (etwa defektes / verrutschtes Transportgut) erkennen und diese in bestimmten Fällen durch den Einsatz von Fehlerbeseitigungsmechanismen selbstständig bereinigen können (etwa durch Aussonderung / Neuanordnung des defekten / verrutschten Transportguts).
– *Stufe 5 (autonom):* Das System ist imstande, in *allen* Situationen die zugewiesene Aufgabe selbstständig zu übernehmen. Das System muss weder überwacht werden, noch wird ein menschlicher Eingriff notwendig, da das System fähig ist, Fehler und Probleme selbstständig zu umgehen oder zu beseitigen.
Beispiel: Einsatz komplexer Fertigungsanlagen, die durch den Einsatz intelligenter Fehlererkennungsmechanismen und zahlreicher Fehlerbeseitigungsmechanismen imstande sind, jegliche auftretenden abnormalen Zustände zu erkennen und zu beseitigen.

1.3 Der Entwicklungsstand automatisierter Systeme

Im Industrie- und Dienstleistungsbereich finden bereits heute schon zahlreiche unterschiedliche automatisierte Systeme Anwendung. Dieser Entwicklungsstand soll im Folgenden zunächst überblicksmäßig und dann an den konkreten Beispielen automatisiertes Straßenfahrzeug und automatisiertes Luftfahrzeug dargestellt werden.

1.3.1 Die Automatisierung in der Industrie

Kapitelübersicht

1.3.1.1 Von der Industrie 1.0 zur Industrie 4.0

Die Automatisierung von Arbeitsvorgängen in der Industrie ist nicht erst eine Erfindung der letzten Jahre, sondern bereits seit der ersten industriellen Revolution (*Industrie 1.0*) zu beobachten, als mithilfe von Wasser- und Dampfkraft mechanische Produktionsanlagen genutzt und die Herstellungsabläufe daher effizienter und mit weniger Personalbedarf ausgestaltet werden konnten.

Die zweite industrielle Revolution (*Industrie 2.0*) folgte sodann bei Beginn des 20. Jahrhunderts, als im Schlachthof von Cincinnati das erste Fließband zum Einsatz kam. Das Fließband ermöglichte erstmals eine neue Form der Massenproduktion und Arbeitsteilung, indem ein Mitarbeiter nichtmehr eine Vielzahl an Arbeitsschritten, sondern nur noch spezifische Handlungsabläufe zu erledigen hatte.

Die heute in der Industrie vorzufindende Automatisierung – insbesondere durch die Robotik – ist indes aber vielmehr ein Produkt der dritten industriellen Revolution (*Industrie 3.0*) zu Beginn der 70er Jahre des 20. Jahrhunderts, als mit der Fortentwicklung der Informations- und Kommunikationstechnik Arbeitsabläufe mithilfe von Computertechnik automatisiert werden konnten. Diese automatisierten IuK-Systeme konnten seitdem beständig weiterentwickelt werden, sodass heutige Industrieroboter eine unüberschaubare Vielzahl an Arbeiten verrichten können. Dies betrifft etwa die Ausführung schwerer Hebe- und Tragarbeiten bei den Automobilherstellern oder die Verrichtung präziser Lötarbeiten bei den Chipherstellern.

Die Industrie erlebt mit der *Industrie 4.0* derzeit bereits ihre vierte industrielle Revolution. Während der Einsatz von automatisierter Robotertechnik, wie bereits dargestellt, schon im Wege der dritten industriellen Revolution Einzug gefunden hat, erfolgt im Rahmen der vierten industriellen Revolution nun eine dezentrale oder zentrale Vernetzung der einzelnen Komponenten und Maschinen. Diese stehen hierdurch in einem permanenten Informationsaustausch zueinander. Die Vernetzung der Einzelkomponen-

ten wird durch den Einsatz intelligenter Algorithmen ergänzt, sodass die einzelnen IT-Systeme die hierbei gewonnenen Informationen auch für den Produktionsprozess gewinnbringend verwerten können. Das betrifft etwa die Meldung über die derzeitige Eigenauslastung des jeweiligen Systems an die anderen Komponenten, die daraufhin die Zustellung weiterer Bauteile besser koordinieren können. So ist beispielsweise denkbar, dass die Lackierstation in der Automobilproduktionshalle die verbleibende Arbeitszeit für das derzeit zu lackierende Bauteil an die Zustellroboter oder die Fließbänder meldet, die daraufhin entweder bereits das nächste zu lackierende Bauteil liefern, oder aber bei noch andauerndem Lackierprozess auf eine andere Lackierstation ausweichen. Diese Vernetzung und „Smartifizierung" zu einer „Smart Factory" wird insbesondere zu einer Steigerung der Produktionsauslastung führen, als hierbei Leerlaufzeiten sowie Materialverschwendung vermieden werden können.

1.3.1.2 Ausgewählte Beispiele der Automatisierung in der Industrie

Mittels der Vernetzung einzelner Produktionsmaschinerie und Arbeitsstationen ist es möglich, ganze Produktionsabläufe – von den Einzelbauteilen zum fertigen Produkt – zu automatisieren. Im Rahmen der bereits aufgezeigten allgemeinen Automatisierungsstufenlehre ist hierbei bereits heute eine Automatisierung auf der Stufe der *Hochautomatisierung* vollständig etabliert, bei der das System Fehler im Produktionsablauf zumindest selbstständig feststellen kann und dann in einen Wartezustand übergeht, bis dieser (durch menschlichen Eingriff) behoben wurde. Doch auch *vollautomatisierte* Industrieanlagen befinden sich heute schon im Praxiseinsatz, welche Fehler im Produktionsablauf nicht nur erkennen, sondern gar selbst und ohne fremde Hilfe beseitigen können.

Als erstes Beispiel können hierbei sog. automatisierte „Flurförderfahrzeuge" oder sonstige automatisierte Fördersysteme angeführt werden, die etwa von der BMW Group oder von ThyssenKrupp eingesetzt werden.[2] Laut Herstellerangaben sind diese automatisierten Systeme dabei imstande, per Lasernavigation geleitet, selbstständig Waren innerhalb eines Werks oder Werksgeländes zu transportieren.[3] Je nach konkreter Ausführung sind diese Förderfahrzeuge dann bereits auf der Stufe der *Vollautomatisierung* oder der *Autonomie* einzuordnen, wenn diese Hindernisse selbstständig erkennen und umfahren können und daher auf keine fremde Hilfe oder Überwachung mehr angewiesen sind.[4]

---

[2] http://www.jungheinrich.de/automatische-foerderzeuge/referenzen-automatische-foerderzeuge/ (abgerufen am 23.12.2016).
[3] http://www.jungheinrich.de/automatische-foerderzeuge/ (abgerufen am 23.12.2016).
[4] Der Hersteller selbst spricht dagegen nur von einer „teilweisen oder vollständigen Automatisierung" außerhalb der hier zugrunde gelegten Automatisierungsstufenlehre, vgl. http://www.jungheinrich.de/automatische-foerderzeuge/ (abgerufen am 23.12.2016).

Weiterhin sind auch sog. automatisierte „Portalroboter“ zu nennen, die zu Be- und Entladearbeiten an Maschinen und Arbeitsstationen eingesetzt werden und hierbei imstande sind, diese Arbeiten auch selbstständig durchzuführen und zu koordinieren. Je nach Ausgestaltung eines solchen Portalroboters, also danach, ob dieser Fehler im Ablauf automatisch erkennen und auch korrigieren kann oder zur Korrektur des Fehlers noch menschlicher Hilfe bedarf, sind auch diese bereits auf der Stufe der *Vollautomatisierung*, zumindest aber auf der Stufe der *Hochautomatisierung*, einzuordnen.

Als drittes Beispiel kann auch das Elektronik- und Gerätewerk der Siemens AG im bayerischen Amberg genannt werden, das aufgrund seiner intelligenten und automatisierten Produktionsanlagen zu den modernsten Werken der Welt zählt.[5] Eine große Herausforderung der Automatisierung ganzer Fabrikationshallen liegt dabei gerade auch in der Lokalisierung und Identifizierung der verschiedenen Bauteile durch die einzelnen Produktionsstationen. Hierzu kommen heute optische zweidimensionale Codes (sog. QR-Codes) zum Einsatz, die auf jedes einzelne Bauteil aufgeklebt oder gedruckt werden.[6] Diese Codes können sodann von zahlreichen intelligenten Kamerasystemen in der Smart Factory erfasst und von der jeweiligen Produktionseinheit interpretiert werden. Zudem werden hierzu häufig auch sog. RFID-Systeme (Radio-Frequency Identification) eingesetzt, deren (meist passive) Sender es aufgrund der kleinen Größe und der minimalen Kosten erlauben, eine Vielzahl an – auch sehr kleinen – Bauteilen zu bestücken. Durch den Einsatz dieser Identifikationstechniken sowie weiterer Automatisierungslösungen konnte auch hier bereits die Stufe der *Vollautomatisierung* erreicht werden.[7]

Neben automatisierten Industrierobotern und Fließbändern kommen in der Industrie weiterhin auch automatisierte Softwareprodukte zum Einsatz, wie etwa die Software „Automic“, die im Kontext der Industrie 4.0 gesamte Produktions- und Lieferketten automatisiert. Hierbei soll etwa bei einem deutschen Sportartikelhersteller künftig ermöglicht werden, dass ein Kunde im Ladengeschäft ein individuell designtes Produkt bestellt und diese Bestellung sodann unmittelbar, also ohne weitere Zwischenstationen und ohne zeitliche Verzögerung, in die Produktionsabteilung weitergereicht und hergestellt wird. Weiterhin soll durch Automic ermöglicht werden, dass im Ladengeschäft verkaufte und im Lager nicht mehr vorhandene Produkte automatisiert nachbestellt werden und insofern Lieferverzögerungen und damit leere Regale vermieden werden können.

Auch automatisierte Straßen- und Luftfahrzeuge werden zukünftig in der Industrie vermehrt eingesetzt werden. Denn gerade bei großen und weitläufigen Produktionsstätten

---

[5] http://www.siemens.com/innovation/de/home/pictures-of-the-future/industrie-und-automatisierung/digitale-fabrik-industrie-4-0.html (abgerufen am 22.12.2016).
[6] http://www.mittelstand-digital.de/MD/Redaktion/DE/PDF/rfid-steuert-produktion-und-logistik-pdf,property=pdf,bereich=md,sprache=de,rwb=true.pdf (abgerufen am 22.12.2016).
[7] Vgl. https://www.merkur.de/wirtschaft/merkel-besuch-siemens-amberg-zr-4758778.html (abgerufen am 23.12.2016).

können mittels automatisierter Transportfahrzeuge Bauteile zwischen den einzelnen Werkshallen schnell und flexibel ausgetauscht werden.

1.3.2 Die Automatisierung im Dienstleistungssektor

Die Entwicklung von Dienstleistungsrobotern, insbesondere sog. „Humanoide“ / „Androide“, also dem menschlichen Körper nachempfundener Roboter, die dem Menschen im Alltag behilflich sind, ist bereits seit den Anfängen der Informations- und Kommunikationstechnologie ein Wunschtraum Vieler. So wurde in dem Film Metropolis etwa schon 1927 ein Humanoide vorgeführt, der einem weiblichen Maschinenmenschen glich. Und bereits 1939 wurde der erste tatsächliche humanoide Roboter „Elektro“ auf der Westinghouse Weltausstellung in New York präsentiert, der sogar einen Wortschatz von 700 Wörtern besaß, selbstverständlich aber noch von einem Menschen ferngesteuert werden musste, also noch keine automatisierten Algorithmen ausführen konnte.

Heute existiert eine Vielzahl an Robotikunternehmen, die Service- und Dienstleistungsroboter für die unterschiedlichsten Einsatzszenarien herstellen. Für den privaten Bereich sind etwa bereits heute in jedem Elektronikfachmarkt automatisierte Staubsauger- oder Wischroboter erhältlich, die ihre Aufgaben bereits *hoch*- oder gar *vollautomatisiert* ausführen können (je nachdem, ob der Roboter auf Hindernisse selbst reagieren kann; bestimmte Hindernisse sind bislang aber noch unüberwindbar (etwa Treppen), sodass die Stufe der *Autonomie* hier noch nicht erreicht werden kann). In jedem Baumarkt sind zudem auch *hoch- oder vollautomatisierte* Rasenmäherroboter erhältlich. Für das Gewerbe wird unter anderem auch „Pepper“, ein 1,20 Meter großer japanischer Roboter, künftig eine Rolle spielen. Dieser soll etwa in Banken und Geschäften Flyer verteilen, Wartende belustigen oder gar Verkaufsgespräche führen. Selbst die Kreuzfahrtschifffflotte AIDA setzt Pepper bereits vereinzelt auf ihren Schiffen ein, wo dieser den Passagieren beim Einchecken und zur Orientierung auf dem Schiff hilft bzw. Ausflugstipps gibt.

Auch im medizinischen Sektor sowie in der Krankenpflege ist der Einsatz von Dienstleistungsrobotern angedacht. So wird etwa am Healthcare Robotics Lab des Georgia Institute of Technology am „PR2“, einem Roboter für die Betreuung Pflegebedürftiger, geforscht. Bislang befindet sich dieser aber noch in der Entwicklungs- und Erprobungsphase.

Doch auch automatisierte Straßen- und Luftfahrzeuge werden zukünftig vermehrt im Dienstleistungssektor Anwendung finden, wenn diese etwa automatisiert Bestellungen ausliefern oder mittels automatisierter Taxis Personen fahrerlos befördert werden.

Bei der Entwicklung von Service- und Dienstleistungsrobotern spielt die Erforschung künstlicher Intelligenz eine Schlüsselrolle. Denn gerade bei diesen ist erforderlich, dass sie sich in den Alltag ihrer Halter oder Kunden bestmöglich integrieren. Aufgrund der Unvorhersehbarkeit alltäglicher Situationen und aufgrund der Unterschiedlichkeit der Persönlichkeit, Vorlieben und Stimmung des jeweiligen Halters oder Kunden können

hierbei nicht alle Szenarien ab Werk einprogrammiert werden. Der Roboter muss insofern vielmehr selbst ein adäquates und optimales Verhalten im Laufe des Betriebs erlernen.

1.3.3 Automatisierte Straßenfahrzeuge

Die Automatisierung des Kfz ist keineswegs eine „Erfindung“ der letzten Jahre. So sprach etwa bereits im Jahre 1958 Frank Rowsome im Magazin „Popular Science“ vom sog. „Auto Pilot“, der schließlich 1962 dann als sog. „Tempomat“ eingeführt wurde. Der Tempomat, aber auch das 1978 entwickelte Antiblockiersystem (ABS), die Antischlupfregelung (ASR) aus den 90er Jahren sowie das Elektronische Stabilitätsprogramm (ESP), stellen bereits die Vorfahren der heutigen Automatisierung im Kfz dar. Diesen frühen *Assistenzsystemen* folgten schließlich der Parklenk- und der Spurhalteassistent, die beim Parken vollständig, beim Fahren auf der Autobahn hilfsweise, die Steuerung über das Lenkrad übernehmen, während der Fahrzeugführer weiterhin die Geschwindigkeit durch Gas geben oder Bremsen kontrollieren muss. Das 2010 eingeführte automatische Notbremssystem kann umgekehrt das Fahrzeug bei erkannten Hindernissen selbstständig abbremsen, während der Fahrer weiterhin die Lenkbewegung kontrolliert.

In Erweiterung des Parklenkassistenten werden seit den 2010er Jahren nunmehr sog. Parkmanöverassistenten in moderne Kfz verbaut, die nicht nur die Lenkbewegung, sondern auch das Beschleunigen und Bremsen beim Einparken übernehmen und in dieser spezifischen Situation also einen Fahrer bereits ersetzen können. Dem Fahrer kommt dabei nur noch eine Überwachungsfunktion zu (*Teilautomatisierung*). Er kann notfalls durch eigene Lenk- oder Bremsimpulse korrigierend eingreifen. Mittlerweile ist es durch das sog. „Schlüsselparken“ sogar möglich, dass sich der Fahrzeugführer während des Parkvorgangs auch außerhalb des Fahrzeugs befindet und diesem mittels des Schlüssels nur noch eine Parklücke aufzeigen muss, in welche das Fahrzeug dann automatisiert einparkt. Ein korrigierendes Eingreifen des überwachenden Fahrzeugführers ist weiterhin per Notstopp möglich, der etwa mit einem Schalter auf dem Schlüssel ausgelöst werden kann. In Zukunft wird durch das sog. „Valet Parking“ auch ein *vollautomatisiertes* Ein- und Ausparken möglich sein. Das Fahrzeug muss hierzu dann nur noch im Einfahrtsbereich eines Parkhauses oder Parkplatzes abgestellt werden. Geleitet durch zahlreiche im Kfz und im Parkhaus angebrachte Sensoren und intelligente Steuerungsalgorithmen kann dieses daraufhin selbstständig einen freien Parkplatz finden, dort einparken und später, nachdem der Fahrzeughalter sein Fahrzeug per Smartphone, Tablet oder Fernbedienung „ruft“, wieder automatisiert ausparken.

Auch beim Stau“assistenten“ ist das automatisierte Kfz mittlerweile in der Lage, in der spezifischen Stausituation die vollständige Kontrolle über die Längs- (vor / zurück) und Querachse (links / rechts) zu übernehmen. Jedoch hat der Fahrzeugführer den Vorgang bislang noch dauerhaft zu überwachen und sicherzustellen, dass er notfalls unverzüglich korrigierend (durch Gegenlenkung oder Bremsen) eingreifen kann (*Teilautomatisierung*). Eine Beschäftigung mit anderen Dingen ist daher derzeit noch nicht

zulässig. Zukünftig soll durch das sog. Staufolgefahren / Fahren im Stau aber auch die Notwendigkeit einer permanenten Fahrzeugüberwachung durch den Fahrzeugführer entfallen und diesem dann ermöglicht werden, sich während der Fahrt mit anderen Dingen zu beschäftigen. Erkennt das System dann die Notwendigkeit einer Steuerungsübernahme durch den Fahrzeugführer, so wird dieser per Warnhinweis darauf aufmerksam gemacht (*Hochautomatisierung*). Dem Fahrzeugführer bleibt dann eine gewisse Übernahmezeit.

Zusammenfassend ist die Automatisierung in Straßenfahrzeugen derzeit also noch auf spezifische Szenarien (Fahren im Stau / Parken) beschränkt. Gerade das Valet Parking ist zudem auf das Vorhandensein einer entsprechenden Infrastruktur in Parkhäusern oder auf Parkplätzen angewiesen. Bis zum Jahre 2020 soll aber auch das Fahren auf der Autobahn automatisiert werden. Einen wichtigen Beitrag zu dieser Fortentwicklung der Kfz-Automatisierung leistet unter anderem die Teststrecke für automatisiertes und autonomes Fahren auf der Bundesautobahn A9, auf der bereits heute schon *hoch- und vollautomatisierte* Fahrfunktionen getestet werden können. Auch das automatisierte Fahren innerhalb der Stadt wird derzeit bereits getestet. Aufgrund der erhöhten Komplexität des automatisierten Fahrens in innerstädtischen Gebieten lassen sich hierbei bisher aber noch keine gesicherten Zukunftsprognosen aussprechen.

Neben dem technischen Entwicklungsbedarf erfordert der Einsatz von automatisierten Fahrfunktionen auch eine Weiterentwicklung des Rechts. Bereits im Juli 2016 hatte der Bundesverkehrsminister Alexander Dobrindt daher eine Reformierung des geltenden Straßenverkehrsrechts (StVG) angekündigt, die am 21.06.2017 mit dem „Achten Gesetz zur Änderung des Straßenverkehrsgesetzes“ schließlich in Kraft getreten ist und zukünftig spezifische Bestimmungen für Kraftfahrzeuge mit hoch- und vollautomatisierten Fahrfunktionen beinhaltet. Als staatenübergreifender Rechtsrahmen dient hierbei das sog. Wiener Übereinkommen von 1968, das hinsichtlich der Ermöglichung von automatisierten Fahrfunktionen bereits mit Wirkung zum 23.03.2016 abgeändert wurde. Es bleiben allerdings sowohl auf nationaler als auch auf internationaler Ebene noch weitere Anpassungen erforderlich.

1.3.4 Automatisierte und autonome unbemannte Luftfahrzeuge (Drohnen)

Unbemannte Luftfahrzeuge sind äußerst anfällig für Umwelteinflüsse wie Wind und Wetter, da sie im Gegensatz zu Straßenfahrzeugen keinen Kontakt zu einem festen Bezugspunkt haben, wie dies bei Straßenfahrzeugen etwa die Straße ist. Diese Umwelteinflüsse bedürfen eines ständigen Gegenlenkens durch die Drohne, damit das Luftfahrzeug stabil in der Luft gehalten werden kann.

Zu diesem Zweck sind so gut wie alle auf dem Markt erhältlichen modernen zivilen Drohnen bereits heute mit zahlreichen hochsensiblen Sensoren und Positionsbestimmungssystemen ausgerüstet. Hierzu gehören unter anderem:

- elektronischer Kompass,
- elektronisches Gyroskop,

- elektronischer Beschleunigungsmesser,
- elektronisches Barometer,
- GPS-Modul.

Je nach Ausgestaltung können zudem weitere Module wie (Ultraschall-)sensoren, Kameras und andere visuelle Positionsbestimmungssysteme verbaut sein, um Hindernisse automatisiert erkennen und umfliegen zu können.

Hierdurch sind moderne Flugdrohnen bereits heute unter anderem in der Lage:

- ihre Position *teilautomatisiert* stabil zu halten,
- Umwelteinflüsse *teilautomatisiert* selbstständig auszugleichen,
- vorgegebene Zielkoordinaten (sog. „Waypoints“) *hoch- oder vollautomatisiert* selbstständig anzufliegen,
- ein vorgegebenes Objekt (sog. „Point of Interest“) *hoch- oder vollautomatisiert* selbstständig zu umfliegen,
- ein vorgegebenes Objekt *hoch- oder vollautomatisiert* zu verfolgen (sog. „Follow Me“-Funktion),
- Hindernisse zu erkennen und *vollautomatisiert* zu umfliegen.

Moderne Flugdrohnen sind also auch heute schon in der Lage, Flüge in spezifischen Situationen automatisiert durchzuführen. Der von der DHL GmbH getestete „Paketkopter“, der bereits erfolgreich Medikamente auf die Nordseeinsel Juist und Pakete auf eine Alm bei Reit im Winkl ausgeliefert hat, ist nur eines von mehreren Beispielen. Auch vom Online-Warenhaus Amazon wird derzeit der „Amazon Prime Air“-Dienst getestet.

Bis Drohnen tatsächlich in unserem Alltag vollautomatisiert oder autonom Lieferungen zustellen oder sonstige Aufgaben übernehmen können, besteht aber auch hier noch erheblicher Forschungsbedarf, der insbesondere auch im sicheren Erkennen und Ausweichen von anderen Flugobjekten und Gegenständen besteht. Gerade in dicht besiedelten städtischen Gebieten kann dies derzeit noch nicht vollumfänglich gewährleistet werden. Neben der Weiterentwicklung der verwendeten Sensorik und der zur Anwendung kommenden softwaregestützten Erkennungs- und Ausweichalgorithmen bedarf es hierbei zukünftig auch neuer Konzepte zur sicheren Integration von Flugdrohnen in den kontrollierten und unkontrollierten Luftraum. Auf der Technologiekonferenz der Deutschen Flugsicherung (DFS) am 15.11.2016 mit dem Titel „Herausforderung Drohnen“ wurde daher ein neues Forschungsprojekt, bestehend aus den Kooperationspartnern Deutsche Flugsicherung DFS, Deutsche Post DHL Group und der Deutschen Telekom AG, gegründet, das sich dieser Aufgabe widmen soll.

Auch hinsichtlich des Einsatzes von automatisierten Drohnen besteht ein Reformierungsbedarf des geltenden Luftverkehrsrechts, das in Deutschland hauptsächlich aus dem Luftverkehrsgesetz (LuftVG), der Luftverkehrsordnung (LuftVO) und der Luftverkehrszulassungsordnung (LuftVZO) besteht. Denn auch nach der Reformierung der LuftVO durch die sog. „DrohnenVO“ (Verordnung zur Regelung des Betriebs von un-

bemannten Fluggeräten v. 30.03.2017) bleibt gem. § 21b Abs. 1 Satz 1 Nr. 1, Abs. 3 LuftVO der Betrieb von unbemannten Luftfahrtsystemen und Flugmodellen außerhalb der Sichtweite des Steuerers weiterhin zulassungspflichtig. Eine Liberalisierung hat die DrohnenVO gem. § 21b Abs. 1 Satz 3 LuftVO hier nur für sog. „FPV-Flüge“ unter 30 Meter Flughöhe vorgesehen, wenn das Fluggerät also etwa per Videobrille gesteuert wird.

1.4 „Smartifizierung“ und Vernetzung zu einer „Smart World“

Nicht nur in der Industrie 4.0 erfolgt derzeit eine Vernetzung bislang isolierter Einzelkomponenten und -systeme zu einem automatisierten und intelligenten Gesamtsystem (sog. „Smart Factory“).

Vielmehr erfährt diese „Smartifizierung“ von Alltagsgegenständen und Prozessen im „Internet of Things“ derzeit und zukünftig eine ubiquitäre Entwicklung, die quasi alle Lebensbereiche betreffen wird (sog. „Smart World“). Bereits heute finden sich in Privatwohnungen schon zahlreiche smarte und vernetzte IT-Komponenten und Geräte wie etwa Smart-TVs, smarte Kühlschränke, sonstige smarte Küchengeräte, smarte Waschmaschinen und eine große Palette an Smart-Home-Geräten wie vernetzte dimmbare Lichtschalter oder zeitgesteuerte Jalousien. Auch unmittelbar am Körper tragen wir bereits das Smartphone und vermehrt auch Smart Watches oder Fitnesstracker. Zukünftig werden noch weitere smarte Bekleidungsgegenstände („Smart Wearables“) hinzukommen. Auch im Straßenverkehr entwickelt sich ein sog. „Smart Traffic“, bestehend aus „Connected Cars“ und einer „Smart Infrastructure“, die miteinander und untereinander vernetzt sind und in einem permanenten Informationsaustausch stehen.

Aufgrund dieser alleserfassenden Vernetzung des Alltags entsteht zunehmend ein digitaler Erlebnisraum, der eine Vielzahl an Komponenten miteinander verbindet. Durch diese „Smartifizierung“ wird dabei auch eine Gesamtautomatisierung unseres Alltags ermöglicht, insofern diese Smart Devices untereinander kommunizieren und bestimmte Prozesse miteinander koordinieren (etwa das Abstellen aller Haushaltsgeräte oder das Aktivieren der Alarmanlage, wenn die Smart Watch an das Smart Home meldet, dass der Nutzer derzeit auswärts unterwegs ist).

1.5 Überblick über die wesentlich betroffenen Rechtsbereiche

Die Automatisierung und Vernetzung von IT-Systemen wirft eine Reihe an Rechtsfragen auf. Zu unterscheiden sind dabei solche, die alle automatisierten Systeme unabhängig von ihrer konkreten Ausgestaltung und Form betreffen und besondere Rechtsfragen, die nur für spezifische automatisierte Systeme relevant werden.

1.5.1 Allgemeine Rechtsbereiche

Kapitelübersicht

1.5.1.1 Datenschutzrecht

Die Automatisierung von IT-Systemen ist nur durch den Einsatz zahlreicher Sensortechnik sowie durch Algorithmen, die die hierbei erhobenen Sensorinformationen verarbeiten, möglich.

Naturgemäß betreffen diese Informationen nicht nur sachbezogene Informationen über das Umfeld des automatisierten Systems, sondern auch personenbezogene oder –beziehbare Informationen über in der Nähe befindliche Personen. Die Erhebung, Verarbeitung und Nutzung von personenbezogenen oder –beziehbaren Informationen unterliegt nach dem deutschen Bundesdatenschutzgesetz (BDSG) einem sog. Verbot mit Erlaubnisvorbehalt. Hiernach ist eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen oder –beziehbaren Daten nur zulässig, wenn entweder eine Einwilligung der betroffenen Person oder aber ein gesetzlicher Rechtfertigungstatbestand vorliegt. Fraglich ist demnach, inwiefern das BDSG den für den Betrieb von automatisierten Systemen notwendigen Datenumgang bereits heute schon berücksichtigt und gestattet.

Zukünftig spielt hier außerdem die Europäische Datenschutzgrundverordnung (EU-DSGVO) eine entscheidende Rolle, die in weiten Bereichen das nationale BDSG ablösen wird.

1.5.1.2 IT-Sicherheitsrecht

In Deutschland existiert bislang kein einheitliches und umfassendes IT-Sicherheitsrecht. Auch das sog. „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz) trifft nur stellenweise Bestimmungen zur adäquaten Absicherung von IT-Systemen für insbesondere die Betreiber kritischer Infrastrukturen.

Im Rahmen der *Informationssicherheit* als Teilgebiet der IT-Sicherheit bleibt daher meist nur ein Rückgriff auf § 9 BDSG in Verbindung mit dem Sicherheitskatalog in der Anlage zum BDSG, der grobe IT-Sicherheitszielsetzungen enthält. Insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt aber auch umfangreiche organisatorische, technische, personelle und infrastrukturelle Handlungsempfehlungen zur Steigerung der IT-Sicherheit bereit (insbesondere die IT-

Grundschutzkataloge). Zukünftig wird auch im Rahmen der IT-Sicherheit die ab 2018 verpflichtende Europäische Datenschutzgrundverordnung (EU-DSGVO) zu beachten sein, die stellenweise auch IT-sicherheitsrechtliche Bestimmungen enthält.

Im Rahmen der *Funktionssicherheit*, als weiteres Teilgebiet der IT-Sicherheit, ist dagegen auf das Produktsicherheitsgesetz (ProdSG) mit seinen Produktsicherheitsverordnungen (ProdSV) sowie auf zahlreiche weitere DIN-, EN-, ISO- und IEC-Richtlinien zurückzugreifen.

1.5.1.3 Haftungsrecht

Werden bei dem Einsatz automatisierter IT-Systeme Personen verletzt oder Sachen beschädigt, stellt sich anschließend stets die Haftungsfrage. Neben spezifischen Haftungsnormen aus dem Straßenverkehrsrecht, dem Luftverkehrsrecht oder dem Datenschutzrecht muss dabei stets auch das allgemeine Vertragsrecht sowie das Deliktsrecht aus dem Bürgerlichen Gesetzbuch (BGB) in Betracht gezogen werden. Neben der eigentlichen deliktischen Haftung kommt darüber hinaus auch ein Schadensersatzanspruch aus § 823 Abs. 2 BGB in Betracht, wenn eine Strafrechtsnorm des StGB und mithin ein sog. Schutzgesetz verletzt wurde.

Gerade bei automatisierten Systemen, bei denen die späteren Handlungsabläufe bereits zum Zeitpunkt der Systementwicklung und –programmierung vorgegeben werden, könnte weiterhin auch der Produkthersteller nach dem Produkthaftungsgesetz verpflichtet sein, entstandene Schäden zu ersetzen. Denn da mit zunehmendem Automatisierungsgrad eine menschliche Steuerung immer weiter zurücktritt, wird die Ursache eines schadensauslösenden Ereignisses zukünftig vermehrt auf den Hersteller zurückzuführen sein. Oft werden gar mehrere Haftungsadressaten in Frage kommen, etwa sowohl der Halter, als auch der Hersteller des automatisierten Systems. Es stellt sich dann die Frage, wie zwischen den verschiedenen Adressaten eine billige und adäquate Haftungsverteilung vorgenommen werden kann.

1.5.2 Besondere Rechtsbereiche

Je nach Art und Weise, Einsatzzweck und konkreter Systemausgestaltung können bei der Entwicklung und bei dem Betrieb eines automatisierten Systems zudem ganz spezifische Vorschriften relevant werden. So ergeben sich bei dem Einsatz eines automatisierten Straßen- oder Luftfahrzeugs etwa besondere Bestimmungen aus dem jeweiligen Fahrzeugzulassungsrecht. Bei dem Einsatz von automatisierten Drohnen im öffentlichen Raum sind je nach Einsatzort etwa auch besondere Bestimmungen des Bundesnaturschutzgesetzes oder des Bundesimmissionsschutzgesetzes zu beachten. Zudem können bei rechtswidrigen Gefährdungen des Luftraums spezifische Normen des StGB relevant werden. Werden zur Realisierung von automatisierten Systemen dagegen Telekommunikationsinfrastrukturen verwendet, kann weiterhin etwa auch das TKG zu beachten sein.

2 Datenschutz und IT-Sicherheit

Zusammenspiel von Datenschutz, Funktionssicherheit und Informationssicherheit

2.1 Begriffsbestimmungen

2.1.1 Datenschutz

Mit dem *Datenschutz* wird das Recht auf informationelle Selbstbestimmung gewährleistet (Art. 2 Abs. 1, Art. 1 Abs. 1 GG), also der Schutz des Einzelnen vor einer rechtswidrigen Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten. Während die IT-Sicherheit Sicherheitsrisiken begegnet, geht es beim Datenschutzrecht also darum, ob Daten legaler Weise erhoben, verarbeitet oder genutzt werden dürfen.

2.1.2 Funktionssicherheit und Informationssicherheit

Der Begriff der IT-Sicherheit ist zu untergliedern in die Teilbereiche *Funktionssicherheit* („Safety“) und *Informationssicherheit* („Security“).

Unter dem Begriff der Funktionssicherheit[8] ist ein IT-System zu fassen, dessen Ist-Funktionalität ohne Abweichungen der erwarteten Soll-Funktionalität entspricht.[9] Vereinfacht gesagt, nimmt ein funktionssicheres System also keine unzulässigen Zustände an[10] – es funktioniert wie vorgesehen, sodass es insbesondere seiner Umwelt (Personen / anderen Sachen / der Natur) keinen Schaden zufügt. Das IT-System soll hinsichtlich seiner Fehlerfreiheit unbedenklich eingesetzt werden können. Insbesondere auf höheren Automatisierungsstufen, auf denen eine dauerhafte Überwachung des Systems durch einen Menschen nicht mehr notwendig ist und das automatisierte System bislang menschlich durchgeführte Arbeitsabläufe eigenständig ersetzt, ist die Gewährleistung von Funktionssicherheit unverzichtbar. Dabei ergibt sich eine Verpflichtung zu einer funktionssicheren Systemausgestaltung bereits aus dem Produktsicherheitsgesetz, das in § 3 Abs. 1 ProdSiG normiert, dass durch ein Produkt die Sicherheit und Gesundheit von Personen nicht gefährdet werden darf. Weiterhin lässt sich eine solche Verpflichtung auch aus dem Strafrecht herleiten, welches beispielsweise die fahrlässige Körperverletzung unter Strafe stellt, wenn also aufgrund eines unsicheren Systems

[8] Vgl. zur funktionalen Sicherheit beim automatisierten Fahren bereits vbw, Automatisiertes Fahren – Datenschutz und Datensicherheit, S. 27 f.
[9] *Eckert*, IT-Sicherheit, 9. Aufl. 2014, S. 6.
[10] *Eckert*, IT-Sicherheit, 9. Aufl. 2014, S. 6.

etwa eine Person verletzt wird. Neben diesen gesetzlichen Verpflichtungen zur funktionssicheren Systemausgestaltung ergibt sich dies aber auch mittelbar aus dem Haftungsrecht, da der Entwickler und Hersteller eines Systems Haftungsfolgen von vornherein vermeiden möchte und daher auf eine funktionssichere Technikgestaltung achten wird.

Mit Informationssicherheit[11] wird dagegen der Schutz der auf einem System gespeicherten und verarbeiteten Informationen gegen fremde Einsicht (Schutz der Vertraulichkeit), Veränderung (Schutz der Integrität) und Löschung (Schutz der Datenverfügbarkeit) verstanden. Ein Unterfall der Informationssicherheit ist dabei die sog. *Datensicherheit*, die explizit den Schutz der auf einem System gespeicherten und verarbeiteten personenbezogenen Daten bezweckt.

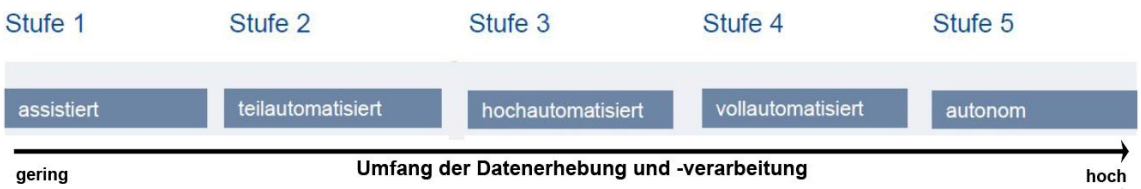
2.2 Zusammenspiel der IT-Sicherheit und des Datenschutzrechts

Die IT-Sicherheit und das Datenschutzrecht sind keine voneinander isolierbaren Komponenten. Vielmehr stehen die Funktionssicherheit (Safety), das Datenschutzrecht (Privacy) und die Informationssicherheit (Security) in ständiger Wechselwirkung zueinander.

Denn zur Erzielung von Funktionssicherheit ist es gerade notwendig, dass zahlreiche Sensordaten über das Umfeld des Systems erhoben und verarbeitet werden. So kann ein automatisiertes Fahrzeug oder ein automatisierter Dienstleistungsroboter sein Umfeld (etwa die in der Nähe befindlichen Personen oder Sachen) nur dann bestmöglich schützen, wenn das System Kenntnis von seiner Umwelt hat (dies geschieht per Erhebung von Sensordaten) und diese Informationen zur Vermeidung von Unfällen und Beschädigungen auch gewinnbringend auswertet (dies geschieht per Verarbeitung der im vorherigen Schritt erhobenen Sensordaten). Mit steigendem Automatisierungsgrad steigt daher auch die Anzahl und der Umfang der notwendigen Datenerhebungen und -verarbeitungen, da die bislang menschlich durchgeführten Handlungen zunehmend durch automatisierte und intelligente Algorithmen ersetzt werden.

[11] Vgl. zur Informationssicherheit beim automatisierten Fahren bereits vbw, Automatisiertes Fahren – Datenschutz und Datensicherheit, S. 28 ff.

Abbildung 2
Umfang der Datenerhebung nach Automatisierungsstufe

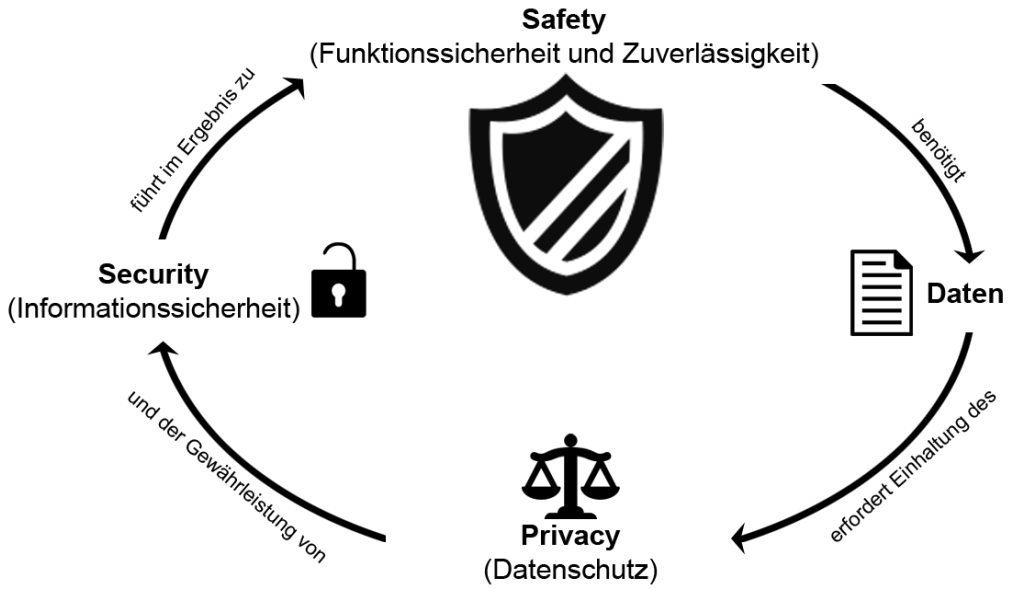


Quelle des Originals: bayme vbm vbw

Eine Erhöhung der *Funktionssicherheit* führt insofern zu dem Dilemma, dass aufgrund zahlreicher Datenerhebungen und -verarbeitungen der *Datenschutz* zunächst verschlechtert wird. Dieses Dilemma kann nur durch eine den Grundsätzen des Datenschutzrechts entsprechende technische Ausgestaltung (bspw. durch die technische Sicherstellung und Realisierung der Grundsätze der Datenvermeidung und der Datensparsamkeit) aufgelöst werden (Privacy by Design).

Diese datenschutzrechtlich legitim erhobenen und gespeicherten Daten müssen sodann hinreichend gegen Fremdzugriff geschützt werden, was Aufgabe der *Informationssicherheit* ist.

Abbildung 3
Zusammenhang zwischen IT-Sicherheit und Datenschutz



Quelle: eigene Darstellung

2.3 Datenschutz in automatisierten Systemen

Es wurde schon gezeigt, dass bereits die Automatisierung von IT-Systemen an sich, insbesondere aber die Gewährleistung von Funktionssicherheit, von der Erhebung und Verarbeitung zahlreicher Sensordaten abhängig ist.[12]

Zu klären ist in diesem Zusammenhang, welche Rechtsgrundlagen für eine solche Datenerhebung und -verarbeitung in Betracht kommen können, welche Arten von Daten hierbei betroffen sind, welche allgemeinen datenschutzrechtlichen Grundsätze existieren und welche konkreten Rechtfertigungsvoraussetzungen für die Nutzung zu Primärzwecken (Realisierung der Automatisierung sowie Gewährleistung der Funktionssicherheit) dabei bestehen.

2.3.1 Rechtsquellen des Datenschutzrechts

Kapitelübersicht

2.3.1.1 Bundesdatenschutzgesetz (BDSG)

In erster Linie kommt bei der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten in Deutschland das Bundesdatenschutzgesetz (BDSG) zur Anwendung. Dieses enthält Bestimmungen sowohl für öffentliche Stellen des Bundes als auch für nicht-öffentliche Stellen. Handelt es sich bei dem datenschutzrechtlich Verantwortlichen nicht um eine öffentliche Stelle des Bundes, sondern um eine öffentliche Stelle eines Landes, kommt dagegen regelmäßig das jeweilige Landesdatenschutzgesetz (in Bayern etwa das Bayerische Datenschutzgesetz, BayDSG) zur Anwendung.

2.3.1.2 Datenschutzrechtliche Spezialgesetze

Nach § 1 Abs. 3 BDSG ist das Bundesdatenschutzgesetz nur insoweit anwendbar, als nicht speziellere Datenschutzgesetze dem BDSG vorgehen. Solche sind etwa das Telemediengesetz (TMG) für die Betreiber von Telemedienangeboten (meist Webseiten)

[12] Zu der allgemeinen rechtlichen Herausforderung von Big Data vgl. *Heckmann*, vbw Studie: Big Data als Chance und Herausforderung für Unternehmen. Zur Unterscheidung zwischen personenbezogenen und sachbezogenen Daten vgl. noch Kapitel 2.3.2.

oder das Telekommunikationsgesetz (TKG) für die Betreiber von Telekommunikationsanlagen. Für die Betreiber von E-Health-Produkten ist weiterhin das Sozialgesetzbuch (SGB) relevant.

Ein eigenständiges, spezifisches Datenschutzrecht für automatisierte Systeme existiert dagegen nicht. Auch hinsichtlich des automatisierten Fahrens oder Fliegens enthalten die Straßen- und Luftfahrtgesetze (insbesondere das StVG und die StVO sowie das LuftVG und die LuftVO) bislang keine spezifischen Datenschutzvorschriften.[13] Daher ist zur datenschutzrechtlichen Bewertung von automatisierten Systemen weiterhin auf die allgemeinen Datenschutzgesetze (BDSG oder EU-DSGVO, siehe sogleich) zurückzugreifen.

2.3.1.3 Europäische Datenschutzgrundverordnung (EU-DSGVO)

Die neue Europäische Datenschutzgrundverordnung (EU-DSGVO - Verordnung (EU) 2016/679) vom 27.4.2016 wird nach einer zweijährigen Übergangszeit am 25.5.2018 in Kraft treten und hat das Ziel, das Datenschutzniveau europaweit zu harmonisieren und an einen hohen Datenschutzstandard anzugleichen.

Die EU-DSGVO entfaltet in ihrem Anwendungsbereich ab dem Zeitpunkt ihres Inkrafttretens Anwendungsvorrang vor den nationalen Datenschutzgesetzen (vor dem BDSG, aber auch vor spezialgesetzlichen Regelungen im TMG, TKG, u.a.). Außerhalb des Anwendungsbereichs der EU-DSGVO bleibt ein Rückgriff auf die weiterhin existenten nationalen Vorschriften möglich. Um dieses Zusammenspiel aus EU-Recht und nationalen Gesetzen für den Anwender zu vereinfachen, wird das nationale Recht künftig auf den verbleibenden Anwendungsbereich hin angepasst werden.

2.3.2 Unterscheidung zwischen personenbezogenen und sachbezogenen Daten[14]

Sowohl das BDSG (§ 4 Abs. 1 BDSG) als auch die datenschutzrechtlichen Spezialgesetze (vgl. etwa § 13 Abs. 1 TMG) sind nur bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten anwendbar.[15] Zu unterscheiden ist demnach, ob die von einem automatisierten System erfassten Sensordaten personenbezogener oder sachbezogener Natur sind.

---

[13] Obgleich das LuftVG etwa schon spezifische Datenschutzvorschriften enthält. Diese betreffen bislang etwa aber nur die Einrichtung einer Flugsicherung (§ 27c LuftVG) und eines Flugwetterdienstes (§ 27e LuftVG), die Durchführung von Vorfeldinspektionen (§ 29 LuftVG) und die Erstellung von Luftfahrtdateien (§ 64 LuftVG).
[14] Vgl. etwa zu den beim automatisierten Fahren anfallenden Arten von Daten bereits das Positionspapier vbw, Automatisiertes Fahren – Datenschutz und Datensicherheit, S. 3 f.
[15] So auch Art. 1 Abs. 1 EU-DSGVO.

Dabei ist zu beachten, dass nach § 3 Abs. 1 BDSG als personenbezogene Daten nicht nur persönliche oder sachliche Verhältnisse einer *bestimmten*, also bereits identifizierten, Person gelten, sondern es hierbei auch ausreicht, wenn die jeweilige Person zumindest *bestimmbar,* also identifizierbar ist (Personenbeziehbarkeit).[16] Unbeachtlich ist dabei, ob eine solche Identifikation tatsächlich stattfindet oder aber angestrebt wird,[17] die theoretische Möglichkeit hierzu ist bereits ausreichend.

Wann eine Person hiernach als identifizierbar gilt, wird im Schrifttum unterschiedlich behandelt. Dabei soll es nach einer Auffassung ausreichen, wenn der Betroffene zwar nicht von der verantwortlichen Stelle selbst, aber von irgendeiner – noch so entfernten – Person oder Stelle erkannt und identifiziert werden könnte (absolute Theorie).[18] Nach einer anderen Auffassung käme es vielmehr auf eine Identifizierbarkeit durch die verantwortliche Stelle selbst an (relative Theorie).[19] Dieser Streitfrage hat sich letztendlich auch der EuGH im Rahmen der Personenbeziehbarkeit von dynamischen IP-Adressen angenommen und dabei einen Mittelweg zwischen beiden Ansätzen gewählt.[20] Nach dem EuGH sei zwar grundsätzlich der Theorie einer relativen Personenbeziehbarkeit zu folgen. Dennoch käme es hierbei nicht zwingend auf die Kenntnisse und Identifizierungsmöglichkeiten der verantwortlichen Stelle selbst an. Vielmehr sei es für eine Personenbeziehbarkeit auch ausreichend, wenn die Identifizierung lediglich mittels Zusatzwissens eines Dritten ermöglicht wird und die verantwortliche Stelle sich an diesen Dritten vernünftigerweise wenden könnte.[21] Als Zusatzwissen zu berücksichtigen sind insofern alle Mittel, „die vernünftiger Weise entweder von dem Verantwortlichen selbst oder einem Dritten eingesetzt werden können, um die betreffende Person zu bestimmen“.[22]

Im Rahmen von automatisierten Systemen, die meist mit zahlreicher Kameratechnik bestückt sind, könnte diese Streitfrage aber ohnehin dahinstehen, wenn die sich in dem Sensorerfassungsbereich des Systems befindlichen Personen im Detail erfasst werden und die dabei erhobenen Daten etwa auch deren Gesichtszüge beinhalten. Denn wird eine Person derart detailliert erfasst, liegt u.U. bereits ein personenbezogenes, also bestimmtes, und nicht erst personenbeziehbares, also bestimmbares, Datum vor.[23] Möchte man dieser weiten Auffassung nicht folgen, so muss zumindest im Rahmen einer Personenbeziehbarkeit berücksichtigt werden, dass die heute frei zur Verfügung stehenden Instrumente, etwa der Face Recognition und der intelligenten Personensuche in sozialen Medien, eine Identifizierung bei einer Personenablichtung leichter ermöglichen als dies etwa bei dynamischen IP-Adressen der Fall ist. Im Ergebnis wird

---

[16] Auch nach Art. 4 Nr. 1 EU-DSGVO liegt ein Personenbezug dann vor, wenn es sich um Daten handelt, die sich auf eine identifizierte oder aber direkt oder indirekt identifizierbare Person beziehen.
[17] Vgl. *Scholz* in: Simitis, BDSG, § 6b BDSG Rn. 67.
[18] *Brink in: Wolff/Brink*, Beck’scher Online-Kommentar Datenschutzrecht, 18. Edition 2016, § 6b BDSG Rn. 40.
[19] So wohl auch *Scholz* in: Simitis, BDSG, § 6b BDSG Rn. 67.
[20] EuGH v. 12.05.2016 – C-582/14 – BeckRS 2016, 81027.
[21] EuGH v. 12.05.2016 – C-582/14 – BeckRS 2016, 81027.
[22] *Schild* in: Wolff/Brink, Beck’scher Online-Kommentar Datenschutzrecht, 18. Edition, Stand 01.11.2016, § 3 Rn. 20.
[23] So etwa *Starnecker*, Videoüberwachung zur Risikovorsorge, S. 126.

daher immer dann, wenn eine Person auf einer Kameraaufzeichnung anhand ihrer Gesichtszüge erkennbar ist, ein personenbezogenes oder zumindest -beziehbares Datum vorliegen, auch wenn die Person der verantwortlichen Stelle bislang noch unbekannt ist.[24] Nur bei Übersichtsaufnahmen aus größerer Entfernung oder bei sonstigen Aufnahmen, die aufgrund einer zu geringen Bildschärfe keine Individualisierung – auch nicht per Zusatzwissen – zulassen, ist ein Personenbezug dann abzulehnen.[25]

Etwas anderes könnte sich nur dann ergeben, wenn das verwendete automatisierte System zur Informationsbeschaffung gar keine solchen Kamerasysteme verwendet, sondern mittels sonstiger, „neutraler" Sensoren (etwa mittels Ultraschall oder kapazitativer Berührungssensoren) ausgestattet ist, die von sich aus nicht imstande sind, personenbezogene Merkmale zu erheben, oder wenn intelligente Kamerasysteme verwendet werden, die immer dann keine Daten erheben, wenn sich eine Person im Erfassungsradius befindet (in diesem Fall stellt das System mittels „neutraler" Sensoren lediglich fest, dass sich *eine* Person im Erfassungsradius befindet, erstellt dann aber keine personenbeziehbare Bild- oder Videoaufnahme). Doch auch in diesen Fällen kann eine Personen*beziehbarkeit* dann doch vorliegen, wenn durch die Heranziehung zusätzlicher Kenntnisse (etwa des Schichtplans) oder zusätzlicher Sensorwerte (sog. Sensorfusion) theoretisch doch noch ein eindeutiger Personenbezug hergestellt werden könnte.

Weiter darf nicht allein aus dem Grund, dass bei der technischen Ausgestaltung eines automatisierten Systems auf den Einsatz von Kameratechnik verzichtet wird, generell und ungeprüft darauf geschlossen werden, dass hierbei nur „neutrale" Sensoren zum Einsatz kämen, die stets nur mittels Zusatzwissens einen Personenbezug zulassen würden. Betrachtet man die Erfassungsdetaildichte und -schärfe von 3D-Lidar-Systemen, die eine Abtastung ihrer Umgebung mittels Laserlicht vornehmen und die häufig beim automatisierten Fahren zum Einsatz kommen, so ist hier – abgesehen von Abweichungen in der Farbdarstellung – nur schwerlich ein signifikanter datenschutzrechtlicher Unterschied zu der Verwendung von Kameras feststellbar.

Eine Datenerhebung mittels optisch-elektronischer Instrumente oder sonstiger Sensoreinrichtungen kann dabei sowohl bewusst und absichtlich (etwa durch die Erfassung der Personen im Umfeld des Systems, um diese zu schützen) oder in Form von unerwünschten Begleitdaten erfolgen. Neben dieser Datenerfassung im Außenbereich des Systems kann etwa im Rahmen von automatisierten Kfz auch eine Datenerhebung im Innenraum (etwa die Anzahl anwesender Passagiere oder Informationen über die Erfüllung der Anschnallpflicht der Insassen, etc.) und auch unabhängig von Sensordaten (etwa die Auswertung des Fahrverhaltens und Generierung eines Fahrprofils) er-

[24] So im Ergebnis wohl auch *Scholz* in: Simitis, BDSG, 8. Aufl. 2014, § 6b BDSG Rn. 67 f. m.w.N.
[25] *Scholz* in: Simitis, BDSG, 8. Aufl. 2014, § 6b BDSG Rn. 68. So auch *Schmid*, K&R 2015, 217, 220.

folgen. Weiterhin können automatisierte Systeme personenbezogene Informationen auch aus bestehenden Datenbanken abrufen, speichern und selbst verarbeiten.

Typisch sachbezogen sind dagegen etwa Systeminformationen zum Zustand und zur Abnutzung des Systems, zum Fortschritt des derzeitigen Arbeitsablaufes, zur Betriebszeit, zur Systemtemperatur, zum Akkustand und zum Energieverbrauch, bei automatisierten Straßen- und Luftfahrzeugen aber auch zu den Wetterbedingungen und zur Witterung. Auch solche zunächst sachbezogenen Informationen können im Einzelfall und insbesondere in Verbindung mit weiteren Informationen aber dann personenbezogene Daten darstellen, wenn sich hieraus dennoch Rückschlüsse auf die rechtliche, wirtschaftliche oder soziale Position des Betroffenen herleiten lassen oder diese Daten zur Beschreibung seiner individuellen Verhältnisse geeignet sind.[26] Kann aus den zunächst sachbezogenen Daten etwa das Fahrverhalten des Fahrzeugführers ausgelesen werden, stellen diese Informationen ebenfalls personenbezogene Daten dar.

2.3.3 Allgemeine Datenschutzgrundsätze

Kapitelübersicht

Das BDSG, die nationalen datenschutzrechtlichen Spezialgesetze, aber auch die EU-DSGVO haben allgemeine datenschutzrechtliche Grundsätze gemeinsam, die sich überwiegend übergesetzlich aus dem Grundrecht auf informationelle Selbstbestimmung oder dem entsprechenden Grundrecht der EU-GRCh ergeben. Die wichtigsten dieser Grundsätze sollen nun, zusammen mit ihrer Relevanz beim Einsatz automatisierter Systeme, dargestellt werden.

Praxistipp

Schon in der Entwicklungsphase eines automatisierten Systems sollte auf eine datenschutzkonforme Technikausgestaltung geachtet werden. Insofern sollen die Datenschutzgrundsätze bereits ab Werk berücksichtigt und implementiert werden (sog. „Privacy by Design“).

[26] *Dammann* in: Simitis, BDSG, 8. Aufl. 2014, § 3 BDSG Rn. 60.

2.3.3.1 Verbotsprinzip mit Erlaubnisvorbehalt

Aus § 4 Abs. 1 BDSG ergibt sich das sog. „Verbotsprinzip mit Erlaubnisvorbehalt". Hiernach ist eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, wenn dies gesetzlich erlaubt ist oder der Betroffene eingewilligt hat. Im Rahmen der weiteren datenschutzrechtlichen Untersuchung wird sich daher stets die Frage stellen, ob für eine spezifische datenschutzrelevante Handlung jeweils eine Einwilligung oder ein gesetzlicher Erlaubnistatbestand vorliegt.

2.3.3.2 Prinzip der Datenvermeidung und Datensparsamkeit

Nach § 3a BDSG sind die „Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen […] an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen". Dieses Prinzip der Datenvermeidung und Datensparsamkeit normiert insofern, dass nicht mehr Daten erhoben oder verarbeitet werden dürfen, als dies tatsächlich erforderlich ist. Zudem sind Daten nach Ablauf dieser Erforderlichkeit unverzüglich zu löschen und diese, wenn möglich und nicht unverhältnismäßig, zu anonymisieren oder zu pseudonymisieren.[27]

Aus diesem Gebot der Datenvermeidung und Datensparsamkeit ergibt sich die Verpflichtung des Entwicklers eines automatisierten Systems, den Umfang der Datenerhebung und –verarbeitung schon im Rahmen der technischen Systemausgestaltung gering zu halten.

Werden per Sensor etwa Informationen über das Umfeld erhoben, sind schon im Zeitpunkt dieser Datenerhebung irrelevante und entbehrliche Informationen zu ignorieren *(Stufe 1)*. Dies bedarf insofern einer Beschränkung der Erfassungsreichweite der Sensoren, um nicht im Rahmen von unerwünschten Begleitdaten auch unnötige personenbezogene Daten zu erheben. Weiterhin befinden sich hierzu derzeit auch intelligente Sensor-/Kamerasysteme in der Entwicklung, die dann, wenn sich ein Mensch im Erfassungsbereich befindet, keine Daten erheben. Dennoch wird sich eine Datenerhebung auf dieser ersten Stufe nicht immer vermeiden lassen, da das automatisierte System entweder auf eine kontinuierliche Datenerhebung, oder aber gerade auf die Erhebung von personenbezogenen oder –beziehbaren Daten angewiesen sein könnte.

Unverzüglich nach dieser Datenerhebung ist der erhobene Datenbestand dann nach dennoch erhobenen, aber unnötigen Daten zu durchsuchen und diese auszufiltern *(Stufe 2)*.

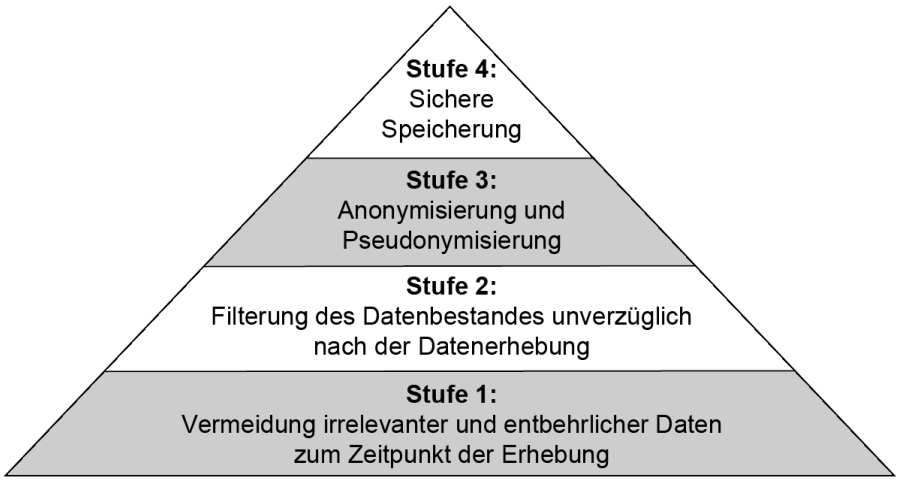
---

[27] Vgl. hierzu auch vbw, Automatisiertes Fahren – Datenschutz und Datensicherheit, S. 19 f.

Relevante personenbezogene Daten, die nicht ausgefiltert werden können, da diese für die weitere Systemausführung notwendig sind, sind – soweit möglich – unverzüglich zu anonymisieren oder zumindest zu pseudonymisieren *(Stufe 3)*.

Die verbleibenden Restdaten sind dann verschlüsselt und gegen fremde Einsicht geschützt zu speichern und unverzüglich zu löschen, wenn diese nicht mehr benötigt werden *(Stufe 4)*.

Abbildung 4
Pyramide der Datenvermeidung bei automatisierten Systemen



Quelle: eigene Darstellung

2.3.3.3 Zweckbindungsgrundsatz

Bei der Nutzung automatisierter Systeme ist zwischen Primär- und Sekundärzwecken zu unterscheiden. Während die Primärzwecke der grundsätzlichen Realisierung des automatisierten Systems sowie der Gewährleistung von Funktionssicherheit dienen, sollen die Daten im Rahmen der sekundären Zwecke auch für darüberhinausgehende Aufgaben (etwa Forschung, Entwicklung, Marketing, Nutzungsberichte etc.) verwendet werden.

Nach dem sog. Zweckbindungsgrundsatz sind bei der Erhebung und Verarbeitung von personenbezogenen Daten die vorher festgelegten Verarbeitungszwecke aber strikt einzuhalten. Dies unterbindet zum einen eine Datenerhebung für unbestimmte Zwecke „auf Vorrat“. Zum anderen wird hierdurch auch eine spätere Zweckänderung erschwert, die dann ggf. nur nach zusätzlicher Einwilligung des Betroffenen möglich ist.

Auch die IT-Sicherheitszielsetzungen der Anlage zu § 9 BDSG sehen insoweit explizit die Einhaltung des Zweckbindungsgrundsatzes vor, da das achte IT-Sicherheitsgebot

der Anlage bestimmt, dass zu unterschiedlichen Zwecken erhobene Daten stets getrennt verarbeitet werden müssen.

2.3.4 Beispiel: Zulässigkeit der Datenerhebung und -verarbeitung nach dem BDSG bei Verwendung einer automatisierten Industriedrohne

Kapitelübersicht

Nach dem Grundsatz des Verbotsprinzips mit Erlaubnisvorbehalt aus § 4 Abs. 1 BDSG ist eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das Gesetz dies erlaubt oder eine Einwilligung des Betroffenen vorliegt. Das Vorliegen dieser Rechtmäßigkeitsvoraussetzungen kann dabei stets nur für den konkreten Einzelfall beurteilt werden. Das Vorgehen bei der datenschutzrechtlichen Rechtmäßigkeitsprüfung soll im Folgenden daher anhand eines solchen konkreten Einzelfalles beispielhaft aufgezeigt werden. Hierfür soll folgendes Szenario zugrunde gelegt werden:

Das Werksgelände eines Industrieunternehmens wird von einer öffentlichen Straße in zwei Teile getrennt. Auf beiden Teilen des Werksgeländes finden sich Produktionsstätten. Zum Transport kleinerer Bauteile von dem einen Werksgelände über die öffentliche Straße hinweg zu dem anderen Werksgelände sollen künftig automatisierte Industriedrohnen eingesetzt werden, die zur Erfassung ihrer Umgebung intelligente Kamerasysteme, also optisch-elektronische Einrichtungen, verwenden.

Datenschutzrechtliche Relevanz erhält dieser Anwendungsfall dadurch, dass die automatisierte Transportdrohne zahlreicher Sensorinformationen (insbesondere durch Kamerasysteme und sonstige optisch-elektronische Einrichtungen) zur 1) Orientierung im Raum, 2) Routenbestimmung, 3) Erkennung und Vermeidung von Hindernissen und 4) zum Schutz von in der Nähe befindlichen Personen und Sachen bedarf.

Da das BDSG sowohl personen*bezogene*, als auch personen*beziehbare* Daten schützt (vgl. § 3 Abs. 1 BDSG sowie Kapitel 2.3.2) ist davon auszugehen, dass sich unter den erhobenen und verarbeiteten Sensorinformationen auch zahlreich datenschutzrechtlich relevante Daten befinden werden. Dies betrifft zumindest personenbeziehbare Informationen über die sich auf den Werksgeländen befindlichen Arbeitnehmer.[28] Doch auch hinsichtlich der Passanten auf dem überflogenen öffentlichen Grundstück ist eine Personenbeziehbarkeit dann zu bejahen, wenn hierbei deren Gesichtszüge oder das sonstige äußere Erscheinungsbild erkennbar aufgezeichnet wird und die Personen daher bestimmt oder mit noch verhältnismäßigem Aufwand bestimmbar sind.[29]

Im Sinne der oben bereits dargestellten „Pyramide der Datenvermeidung bei automatisierten Systemen“ sind dabei technisch alle möglichen und verhältnismäßigen Maßnahmen einzusetzen, um das Anfallen von personenbezogenen Daten bereits zum Zeitpunkt der Erhebung zu vermeiden (Stufe 1). Trotz dieser ersten Schutzmaßnahme werden von der Drohne aber zahlreiche personenbezogene und –beziehbare Daten erhoben werden, die anschließend teilweise gefiltert (Stufe 2) und anonymisiert (Stufe 3) werden. Bereits diese anfängliche Datenerhebung von personenbezogenen oder -beziehbaren Daten, auch wenn diese Daten später wieder ausgefiltert oder anonymisiert werden, bedarf einer gesetzlichen Grundlage oder einer Einwilligung der Betroffenen. Weiterhin verbleiben auch nach der Filterung und Anonymisierung personenbezogene oder -beziehbare „Restdaten“ bei der Drohne, wenn die Drohne gerade diese zur Erledigung ihrer Aufgaben benötigt. Diese Datenverarbeitung und –nutzung bedarf einer weiteren gesetzlichen Grundlage oder einer Einwilligung der Betroffenen.

2.3.4.1 Bezüglich der Arbeitnehmer auf dem Werksgelände

2.3.4.1.1 Datenschutzrechtlicher Erlaubnistatbestand zur Datenerhebung und -verarbeitung nach dem BDSG

Die Datenerhebung und -verarbeitung der Arbeitnehmerdaten auf dem Werksgelände könnte zunächst durch einen gesetzlichen Erlaubnistatbestand des BDSG gerechtfertigt sein. Wäre ein solcher Erlaubnistatbestand einschlägig, bedürfte es keiner zusätzlichen Einwilligung der Betroffenen. Für die Datenerhebung und Datenverarbeitung der Industriedrohne kommen im Verhältnis zu den Arbeitnehmern sowohl § 6b BDSG, der eine spezielle Ermächtigungsgrundlage für die Beobachtung mittels optisch-elektronischer Einrichtungen enthält, sowie § 32 BDSG, der eine spezielle Ermächtigung für den Datenumgang im Beschäftigungsverhältnis vorsieht, in Betracht.

---

[28] Die hierbei erhobenen und verarbeiteten Daten enthalten zumindest die personenbeziehbaren Informationen, dass sich eine bestimm*bare* Person zu einer bestimmten Zeit an einem bestimmten Ort aufgehalten hat.
[29] Vgl. *Scholz* in: Simitis, BDSG, § 6b BDSG Rn. 67. Dazu bereits Kapitel 2.3.2.

Hinsichtlich des § 6b BDSG muss aber bereits festgestellt werden, dass hierbei dem Wortlaut nach nur „öffentlich zugängliche Räume“ betroffen sind, wovon im Rahmen eines durch Mitarbeiterausweise und Zugangskontrollen gesicherten Betriebsgeländes grundsätzlich nicht ausgegangen werden kann. Wäre das betreffende Werksgelände allerdings auch für unbekannte, nicht-angestellte Dritte zugänglich, würde sich diese Beurteilung ändern und es wären die Voraussetzungen des § 6b BDSG zu erfüllen, wenn zudem auch eine „Beobachtung“ des öffentlich zugänglichen Raums vorliegen würde. Eine solche Beobachtung und mithin eine „Videoüberwachung“ i.S.d. § 6b BDSG kann insofern zwar nur dann bejaht werden, wenn die Einsichtnahme in den öffentlichen Raum über einen gewissen Zeitraum erfolgt.[30] Da das ordnungsgemäße Funktionieren einer automatisierten Industriedrohne aber von einer kontinuierlichen Umgebungserfassung abhängig sein wird, ist hiervon jedoch auszugehen.

Für Drohnenflüge auf dem nicht-öffentlichen Werksgelände müsste die Erhebung und Verarbeitung der automatisiert ausgewerteten Bilddaten also auf § 32 BDSG gestützt werden. Nach § 32 Abs. 1 BDSG dürfen personenbezogene Daten eines Beschäftigten dann erhoben, verarbeitet oder genutzt werden, wenn dies unter anderem für die Durchführung des Beschäftigungsverhältnisses *erforderlich* ist.

Durch das Kriterium der Erforderlichkeit wird dabei erneut deutlich, dass an die technische Ausgestaltung der automatisierten Industriedrohne hohe Anforderungen hinsichtlich der Datensparsamkeit und Datenvermeidung zu stellen sind. Zudem wurde auch im Kontext von Videoüberwachungsmaßnahmen am Arbeitsplatz, die jedenfalls technisch mit den hier in Rede stehenden datenerhebenden und –verarbeitenden automatisierten Systemen vergleichbar sind, im Schrifttum und in der Rechtsprechung bereits ausgeführt, dass hierbei § 32 Abs. 1 Satz 1 BDSG äußerst restriktiv anzuwenden ist. Vorliegend ist aber zu bedenken, dass der Einsatz der Kameratechnik in der Industriedrohne lediglich dem ordnungsgemäßen Funktionieren der Drohne und sogar dem Schutz des Arbeitnehmers dient, eine Überwachung also weder angedacht ist noch tatsächlich stattfindet. Der Kameraeinsatz bei Industriedrohnen ist insofern doch nicht mit einer typischen Videoüberwachung eines Betriebes vergleichbar, sodass der Eingriff in das Recht auf informationelle Selbstbestimmung des Arbeitnehmers, im Vergleich zur tatsächlichen Videoüberwachung, hier geringer ausfällt.

Gerade hinsichtlich der Erfüllung der Tatbestandskriterien des § 32 Abs. 1 Satz 1 BDSG kommt es auf eine strikte Einhaltung der oben dargestellten *Pyramide der Datenvermeidung bei automatisierten Systemen* an. Je nach Art und Weise des konkret eingesetzten automatisierten Systems sowie abhängig von dem Ausmaß der dabei durchgeführten Datenerhebung und –verarbeitung wird in entsprechenden Fällen hilfsweise aber auf eine Einwilligung des Arbeitnehmers zurückgegriffen werden müssen.

---

[30] Vgl. *Schmid*, K&R 4/2015, 217, 221.

2.3.4.1.2 Einwilligung in die Datenerhebung und -verarbeitung

Die Voraussetzungen für die Wirksamkeit einer datenschutzrechtlichen Einwilligung ergeben sich aus § 4a BDSG. Demnach muss eine solche Einwilligung zunächst auf einer freien Entscheidung des Betroffenen beruhen. Zudem sind die Betroffenen auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen. Im Allgemeinen lässt sich daraus ableiten, dass eine Einwilligung insbesondere freiwillig, informiert und bestimmt erteilt werden muss.

Eine solche Einwilligungslösung ließe sich zunächst innerbetrieblich – etwa im Rahmen einer von den Angestellten zu unterzeichnenden Betriebsvereinbarung – in Erwägung ziehen. In der Rechtswissenschaft umstritten ist aber, ob eine solche Einwilligung den hierfür notwendigen Tatbestand der „Freiwilligkeit“ erfüllen kann, als sich die Arbeitnehmer stets in einer gewissen Über- / Unterordnungsposition befinden.

Die arbeitnehmerdatenschutzrechtliche Relevanz verdeutlicht auch der hier in Rede stehende Anwendungsfall: Besonders bei der Kameraerfassung von Arbeitnehmern entsteht für diese schnell eine gewisse Drucksituation – da diese Art der Datenerhebung (auch wenn dies tatsächlich nicht gegeben ist) einen gewissen Überwachungscharakter besitzt, welchem der Arbeitnehmer durchgängig ausgeliefert ist.

Wie bereits erläutert wurde, dient der Einsatz der optisch-elektronischen Einrichtungen in der Industriedrohne aber lediglich dem ordnungsgemäßen Funktionieren der Drohne und gar dem Schutz der Arbeitnehmer. Eine Überwachung ist dabei also weder angedacht, noch findet eine solche tatsächlich statt, sodass der Eingriff in das Recht auf informationelle Selbstbestimmung des Arbeitnehmers hierbei im Vergleich zur herkömmlichen Videoüberwachung geringer ausfällt. Dieser Eingriff wird unter strikter Beachtung der oben bereits dargestellten *Pyramide der Datenvermeidung bei automatisierten Systemen* weiter minimiert, indem die personenbezogenen Arbeitnehmerdaten alsbald anonymisiert oder wieder vom System gelöscht werden, wenn diese für das Funktionieren des Systems nicht mehr relevant sind. Dies kann unter Umständen auch innerhalb weniger Sekunden bereits der Fall sein.

Da das Bundesverfassungsgericht im Rahmen der sog. „automatisierten Kfz-Kennzeichenerfassung“ in einem ähnlich gelagerten Fall sogar entschieden hat, dass bei einer solchen kurzzeitigen und automatisierten Auswertung personenbezogener Daten gar kein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt, muss im vorliegenden Sachverhalt bei einem zumindest derart geringen Eingriff jedenfalls eine Einwilligung des Arbeitnehmers möglich sein. Auch wenn diese - vielfach kritisierte – Auffassung des Bundesverfassungsgerichts nicht ohne Zweifel übernommen werden sollte, kann sie also dennoch als gewichtiges Argument für die Zulässigkeit einer Einwilligung herangezogen werden. Ist sichergestellt, dass das automatisierte System keine Überwachungsgefahr darstellt und werden die stattfindenden Daten-

erhebungs- und Datenverarbeitungsschritte ausführlich in der Einwilligungserklärung erläutert, so kommt eine Zustimmung der Arbeitnehmer in entsprechende Anwendungsszenarien also durchaus in Betracht.

2.3.4.2 Bezüglich der Passanten auf dem öffentlichen Terrain

2.3.4.2.1 Datenschutzrechtlicher Erlaubnistatbestand zur Datenerhebung und -verarbeitung nach dem BDSG

Für Passanten und Dritte, die sich wie im Anwendungsbeispiel in öffentlich zugänglichen Räumen bewegen, ergibt sich die Zulässigkeit der Datenerhebung und -verarbeitung aus § 6b BDSG.[31] Auch hier ist eine Videoüberwachung zwar nur dann zulässig, wenn sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und die schutzwürdigen Interessen der Betroffenen nicht überwiegen. Das Tatbestandskriterium der berechtigten Interessen umfasst dabei aber jedes tatsächliche Interesse wirtschaftlicher oder ideeller Natur und damit auch eigene Geschäftszwecke (hier der Transport von Bauteilen auf das angrenzende Werksgelände und insofern die Aufrechterhaltung des ordnungsgemäßen Betriebs des Unternehmens).[32] Die Einhaltung des gesetzlichen Tatbestands ist insofern keineswegs ausgeschlossen, sondern bei Beachtung bestimmter technischer und rechtlicher Erforderlichkeits- und Verhältnismäßigkeitsmaßstäbe durchaus erfüllbar. Bei Drohnenflügen über eine öffentliche Straße müsste etwa die technische Gestaltung der Drohne so konzipiert sein, dass bei sämtlichen Datenerhebungs- und Datenverarbeitungsschritten der Eingriff in die Rechte der Betroffenen möglichst gering gehalten wird und nur insoweit geschieht, wie dies für die ordnungsgemäße Funktion der Drohne zwingend notwendig ist. Dies kann erneut durch strenge Umsetzung der bereits dargestellten Pyramide der Datenvermeidung bei automatisierten Systemen erfolgen.

Juristisch ist dabei allerdings nach wie vor umstritten, wie die in § 6b Abs. 2 BDSG vorgesehene Hinweispflicht bei mobilen Kamerasystemen erfüllt werden kann. Hält man sich vor Augen, dass intelligente automatisierte Transportdrohnen künftig in der Lage sein werden, ihre Flugrouten dynamisch zu generieren (etwa aufgrund unterschiedlicher Wetter-/Windbedingungen), ist fraglich, ob statisch aufgestellte Hinweisschilder zur Umsetzung der Hinweispflicht hierbei geeignete Maßnahmen sein können.

---

[31] Als Voraussetzung gilt hierfür erneut, dass die Einsichtnahme der Drohne in den öffentlichen Raum mit einer gewissen Zeitdauer erfolgt („Beobachtung“) und mithin eine „Videoüberwachung“ im Sinne der Vorschrift vorliegt. Wie oben bereits erläutert wurde, ist aber davon auszugehen, dass das ordnungsgemäße Funktionieren einer automatisierten Industriedrohne von einer kontinuierlichen Umgebungserfassung abhängig sein wird und das Tatbestandsmerkmal mithin vorliegt.

[32] Vgl. *Brink*, Wolff/Brink, Beck’scher Online-Kommentar Datenschutzrecht, 17. Edition, § 6b BDSG Rn. 48 m.w.N.

2.3.4.2.2 Einwilligung in die Datenerhebung und -verarbeitung

Da es sich bei Passanten zumeist um unbekannte Dritte handelt, ist eine allgemeine Einwilligungslösung hier schon faktisch unmöglich. Nicht legitim wäre dabei auch, auf der Straße entsprechende Hinweisschilder aufzustellen und dann anzunehmen, dass der Passant, der die Straße dennoch betritt, in die Datenerhebung und –verarbeitung durch das Betreten konkludent einwilligt.[33] Eine datenschutzrechtliche Einwilligung muss, wie bereits ausgeführt, stets freiwillig erfolgen, was dann regelmäßig nicht gegeben ist, wenn hierbei ein faktischer Zwang (hier: Entzug der Möglichkeit, eine öffentliche Straße zu nutzen) ausgeübt wird.

2.4 Funktionssicherheit (Safety) automatisierter Systeme

Naturgemäß sind die technischen Anforderungen an die Funktionssicherheit eines automatisierten Straßenfahrzeugs anders als etwa bei einem automatisierten Luftfahrzeug und erneut anders bei einem automatisierten Rasenmähroboter. Die zur Erzielung von Funktionssicherheit notwendigen Maßnahmen und Konstruktionsvorschriften sind insofern höchstgradig einzelfall- und systemabhängig und lassen sich daher nicht pauschal für alle automatisierten Systeme verallgemeinern. Vielmehr sind hierbei stets die spezifischen Gefahren und Eigenheiten des jeweiligen Systems zu berücksichtigen. Auch im Rahmen dieses Gutachtens können daher nicht alle für ein spezifisches automatisiertes System in Betracht kommenden Vorschriften aufgeführt werden. Vielmehr soll dem Leser lediglich ein (nicht abschließender) Überblick über die denkbaren Rechtsnormen gegeben werden.

Es ist weiterhin darauf hinzuweisen, dass der Normen- und Gesetzgeber oftmals nicht zwischen den Begriffen der Funktionssicherheit und der Informationssicherheit unterscheidet. Vielmehr wird hierbei meist auf den unpräzisen Begriff der IT-Sicherheit zurückgegriffen. Eine Abgrenzung zwischen Normen, die die Gewährleistung von Funktionssicherheit bezwecken und Normen, die die Gewährleistung von Informationssicherheit bezwecken ist insofern meist nicht trennscharf möglich. In der folgenden differenzierten Darstellung wird daher stets auf den schwerpunktmäßigen Normzweck abgestellt.

2.4.1 ProdSG und ProdSV

Hinsichtlich der Sicherheit neu auf den Markt kommender Produkte kommt als zentrale Norm zunächst das Produktsicherheitsgesetz (ProdSG) zur Anwendung. Nach § 3 Abs.

---

[33] Vgl. weiterhin bereits oben in Kapitel 2.3.4.2.1 zu der Problematik, dass intelligente automatisierte Flugdrohnen künftig ihre Flugrouten dynamisch bestimmen können werden und es daher ohnehin fraglich ist, ob mit statisch aufgestellten Hinweisschildern Rechtssicherheit erzielt werden kann.

1 ProdSG darf ein Produkt, das einer oder mehrerer der Rechtsverordnungen nach § 8 Abs. 1 ProdSG unterliegt, nur dann auf dem Markt bereitgestellt werden, wenn es die in dieser Rechtsverordnung vorgesehenen Anforderungen erfüllt und die Sicherheit und Gesundheit von Personen oder sonstiger in den Rechtsverordnungen aufgeführter Rechtsgüter bei bestimmungsgemäßer oder vorhersehbarer Verwendung nicht gefährdet. Durch diese nach § 8 ProdSG ergehenden Produktsicherheitsverordnungen (ProdSV) können insbesondere auch Anforderungen an die Beschaffenheit von Produkten geregelt werden. Die ProdSV setzen dabei meist auch europäische Produktrichtlinien in nationales Recht um. Zum Zeitpunkt dieser Ausarbeitung existieren bereits 14 ProdSV, die allesamt nach spezifischen Themengebieten verfasst sind. Für das Inverkehrbringen von automatisierten Systemen kann dabei insbesondere die 1. ProdSV (Verordnung über das Inverkehrbringen elektrischer Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen) und die 9. ProdSV (Maschinenverordnung) in Betracht kommen. Eine spezifische ProdSV für automatisierte Systeme existiert zum Stand dieser Ausarbeitung dagegen nicht.

Auch außerhalb der ProdSV bleibt das ProdSG weiterhin relevant. Denn in § 3 Abs. 2 ProdSG bestimmt das Produktsicherheitsgesetz weiter, dass auch ein Produkt, dass nicht dem § 3 Abs. 1 ProdSG und daher keiner ProdSV unterliegt, nur dann auf dem Markt bereitgestellt werden darf, wenn es bei bestimmungsgemäßer oder vorhersehbarer Verwendung die Sicherheit und Gesundheit von Personen nicht gefährdet. Hierbei sind nach § 3 Abs. 2 Nr. 1 ProdSG auch die Eigenschaften des Produkts und nach Nr. 2 zudem die Einwirkungen des Produkts auf andere Produkte, zu berücksichtigen.

2.4.2 IT-Sicherheitsstandards

Neben den ProdSV können weiterhin eine Vielzahl an technischen Regelungen in den diversen und äußerst spezifischen DIN-, EN-, IEC-, ISO- und TC-Standards festgeschrieben sein, die im Folgenden beispielhaft aufgeführt werden sollen. Technische Normen als allgemein anerkannte Regeln der Technik entfalten dabei zunächst zwar keine direkte Bindungswirkung. Eine mittelbare Bindungswirkung kann sich aber dann ergeben, wenn das einschlägige Fachrecht etwa die Einhaltung des Standes der Technik voraussetzt oder aber zur Vermeidung von Haftungsfolgen dem späteren Vorwurf der Fahrlässigkeit durch die Umsetzung des geltenden Technikstandes vorgewirkt werden soll.

Je nach Art und Weise sowie dem Einsatzzweck des automatisierten Systems betrifft dies etwa die EN 61131, die sich mit den Grundlagen speicherprogrammierbarer Steuerung befasst, sowie EN 61499 als Erweiterung für verteilte Steuerungen. In der DIN EN ISO 13482:2014-11 sind Sicherheitsanforderungen für persönliche Assistenzroboter normiert. Hinsichtlich der Sicherheitsanforderungen von Industrierobotern ist weiterhin die DIN EN ISO 10218-1 sowie die DIN EN ISO 10218-2 zu beachten. Die ISO/TS 15066 beinhaltet gar spezifische Anforderungen an Industrieroboter, die in einem kollaborativen Betrieb mit Menschen stehen sollen. Die ISO/IEC 15408 enthält dagegen generelle funktionale Sicherheitsanforderungen für IT-Produkte und IT-Systeme. Weiterhin kann auch die Norm ISO 9787:2013, die die Koordination von Ro-

botern betrifft, und im Rahmen der Industrie 4.0 auch die Norm ISO/IEC 24771:2014 hinsichtlich der Vernetzung und des Informationsaustauschs zwischen einzelnen Industriekomponenten, beachtlich sein. Im Rahmen von industriellen Kommunikationsnetzen und automatisierten Industriekomponenten ist weiterhin die IEC 62443-Reihe (vormals ANSI/ISA99) relevant.[34] Hinsichtlich sicherheitsrelevanter elektrischer und elektronischer Systeme in Kfz ist weiterhin etwa ISO 26262 zu berücksichtigen. Bei dem Einsatz von intelligenten Transportsystemen ist zudem auch der Standards-Katalog ISO/TC 204 zu beachten, der eine ganze Palette an zu beachtenden Standards und Normen zu diesem Einsatzzweck vorsieht. Darüber hinaus existieren noch zahlreiche weitere spezifische zu beachtende Standards und Normen.[35]

2.4.3 MPG

Gerade dann, wenn automatisierte Systeme im medizinischen Bereich eingesetzt werden (etwa zur Betreuung von Pflegebedürftigen oder Kranken), stellen sich besonders hohe Anforderungen an die Funktionssicherheit des Systems, da hierbei ein besonders vorsichtiger und sensibler Umgang notwendig ist und Produktfehler insofern zu schweren Personenverletzungen führen können. Hierbei ist dann zuvorderst das Medizinproduktegesetz (MPG) zu beachten.

2.4.4 ArbSchG und TRBS

Während insbesondere das ProdSG und die sich daraus ergebenden ProdSV Regelungen für das *Inverkehrbringen* von Produkten beinhalten und insofern von dem Entwickler und dem (Zwischen-)händler eines Produkts zu beachten sind, könnten sich für den das automatisierte System einsetzenden Unternehmer auch Pflichten aus dem Arbeitsschutzgesetz (ArbSchG), der Betriebssicherheitsverordnung (BetrSichV) sowie aus den technischen Regeln für die Betriebssicherheit (TRBS) ergeben.

2.4.5 IT-Sicherheitsgesetz

Spezialgesetzlich ist das neue *IT-Sicherheitsgesetz* (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 17.7.2015) zu nennen, das grundsätzlich aber nur auf die Betreiber kritischer Infrastrukturen Anwendung findet. Solche kritischen

---

[34] Besonders relevant werden hierbei die beiden Teile IEC62443-3-1 und IEC62443-3-3 (*Security technologies for industrial automation and control systems* sowie *Security for industrial process measurement and control – network and system security*) sein.

[35] Vgl. etwa nur DIN EN ISO 11354 (Fortgeschrittene Automatisierungstechnologien und deren Anwendung - Anforderungen für das Erreichen einer Prozessinteroperabilität in Fertigungsunternehmen), DIN EN 62714 (Datenaustauschformat für Planungsdaten industrieller Automatisierungssysteme) oder DIN EN ISO 12813:2016-04 (Elektronische Gebührenerhebung - Kommunikation zur Übereinstimmungsprüfung für autonome Systeme).

Infrastrukturen sind nach § 2 Abs. 10 BSIG „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Welche Betreiber dieser Sektoren nun tatsächlich als kritische Infrastrukturen im Sinne des § 2 Abs.10 BSIG gelten, wurde gem. §§ 2 Abs. 10, 10 Abs. 1 BSIG per Rechtsverordnung des Bundesministeriums des Innern bestimmt.[36] Das IT-Sicherheitsgesetz stellt dabei nur ein Artikelgesetz dar, das zahlreiche bereits vorher bestehende Gesetze an den neuen Rechtsstand anpasst. Dies betrifft etwa das bereits angesprochene BSI-Gesetz (BSIG), aber auch zahlreiche weitere Spezialgesetze wie etwa das Atomgesetz (AtG), das Energiewirtschaftsgesetz (EnWG), das Telekommunikationsgesetz (TKG) oder das Telemediengesetz (TMG). Gerade in diesen Spezialgesetzen wurden durch das IT-Sicherheitsgesetz dann zudem auch erhöhte IT-Sicherheitsanforderungen für solche Adressaten erlassen, die gerade keine Betreiber kritischer Infrastrukturen sind (vgl. etwa § 13 Abs. 7 TMG, der auf alle Telemediendiensteanbieter Anwendung findet).

Die Betreiber kritischer Infrastrukturen haben dabei künftig gem. § 8a Abs. 1 BSIG „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der *Verfügbarkeit*, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind“. Bereits aus dem Wortlaut der Norm ergibt sich, dass das IT-Sicherheitsgesetz demnach sowohl die Gewährleistung der Funktionssicherheit als auch der Informationssicherheit bezweckt. Im Kontext von automatisierten Systemen kann das IT-Sicherheitsgesetz dann eine Rolle spielen, wenn ebensolche Betreiber kritischer Infrastrukturen automatisierte Systeme zur Erledigung ihrer Aufgaben einsetzen. Dann können die nach § 8a Abs. 1 BSIG geforderten organisatorischen und technischen Vorkehrungen auch die Ausgestaltung der automatisierten Systeme selbst betreffen.

Nach § 8a Abs. 2 BSIG können zur Erfüllung dieser Pflichten branchenspezifische Sicherheitsstandards mit konkreten Maßnahmenkatalogen vorgeschlagen und aufgestellt werden. Das BSIG enthält, wie bereits das BDSG, dagegen keine konkreten Handlungsempfehlungen. Nach § 8a Abs. 3 BSIG muss in Form von Sicherheitsaudits, Prüfungen oder Zertifizierungen regelmäßig auch eine Erfüllung dieser Pflichten nachgewiesen werden.

[36] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) v. 22.04.2016, BGBl I S. 958 ff.

2.4.6 Gewährleistung der Funktionssicherheit durch das Zulassungsrecht

Zur Sicherstellung und zum Nachweis, dass die notwendigen Maßnahmen zur Gewährleistung von Funktionssicherheit bei automatisierten Straßen- oder Luftfahrzeugen eingehalten wurden, dient das Fahrzeugzulassungsrecht.

Die entsprechenden Vorschriften finden sich für Straßenfahrzeuge in der Fahrzeugzulassungsverordnung (FZV) und für Luftfahrzeuge in der Luftverkehrszulassungsordnung (LuftVZO). Bei Luftfahrzeugen wird hierbei zwischen einer Musterzulassung (vgl. §§ 1 ff. LuftVZO) und einer Verkehrszulassung (vgl. §§ 6 ff. LuftVZO) unterschieden. Während die Musterzulassung die Funktionssicherheit neuer Flugzeugmodelle, also ganzer Baureihen, sicherstellt, wird die Verkehrszulassung bei der anschließenden Einzelzulassung eines Luftfahrzeugs relevant.

Hinsichtlich des Zulassungsrechts für automatisierte Straßenfahrzeuge sind weiterhin etwa das *Wiener Übereinkommen* (Übereinkommen über den Straßenverkehr v. 8.11.1968) in seiner neuesten Fassung (letzte Änderungen des Wiener Übereinkommens in Deutschland vom 23.03.2016), das zur Umsetzung des Übereinkommens in nationales Recht hierfür notwendige Transformationsgesetz sowie weitere EU-Richtlinien (etwa RL 2007/46/EG und neuere EU-RL) und ergänzende ECE-Normen zu beachten.

2.5 Informationssicherheit (Security) automatisierter Systeme

Auch hinsichtlich der Informationssicherheit von IT-Systemen existiert bislang kein einheitlicher Rechtsrahmen. Vielmehr sind hierbei erneut eine Vielzahl an Rechtsnormen zu beachten, wobei nochmals darauf hingewiesen werden muss, dass eine Abgrenzung zwischen Rechtsnormen, die die Gewährleistung der Funktionssicherheit bezwecken und Rechtsnormen, die die Gewährleistung der Informationssicherheit bezwecken, nicht trennscharf vorgenommen werden kann und daher jeweils lediglich auf den schwerpunktmäßigen Normzweck abgestellt wird.

Praxistipp

Schon in der Entwicklungsphase eines automatisierten Systems sollte auf eine sichere Technikausgestaltung geachtet werden. Insofern sollen die IT-Sicherheitsgrundsätze bereits ab Werk bestmöglich berücksichtigt und implementiert werden (sog. „Security by Design“).

2.5.1 § 9 BDSG i.V.m. der Anlage zum BDSG

§ 9 BDSG i.V.m. der Anlage zum BDSG könnte als zentrale Informationssicherheitsnorm bezeichnet werden. § 9 BDSG findet auf alle öffentlichen und nicht-öffentlichen Stellen Anwendung, die personenbezogene Daten erheben, verarbeiten oder nutzen. Diese haben gem. Satz 1 dieser Vorschrift alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um insbesondere die in der Anlage zum BDSG genannten Anforderungen zu gewährleisten. § 9 Satz 2 BDSG stellt ergänzend klar, dass diese Maßnahmen nur dann erforderlich und zu treffen sind, wenn ihr Aufwand auch in einem angemessenen Verhältnis zu dem angestrebten Zweck steht. Diese Ausnahmeregelung kann insbesondere bei kleineren und wirtschaftlich schwächeren Unternehmen relevant werden, wenn manche Maßnahmen diese wirtschaftlich oder organisatorisch überfordern würden.

Die Anlage zum BDSG, auf die sich der § 9 BDSG bezieht und die eigentlich dessen Konkretisierung dient, enthält acht IT-sicherheitsrechtliche Zielbestimmungen zu den Bereichen:

- räumliche *Zutrittskontrolle* zu Datenverarbeitungsanlagen,
- *Zugangskontrolle* hinsichtlich der unberechtigten Nutzung von Datenverarbeitungsanlagen,
- *Zugriffskontrolle* hinsichtlich des Auslesens, Kopierens, Veränderns oder Entfernens fremder Daten auf dem System,
- *Weitergabekontrolle* hinsichtlich des Auslesens, Kopierens, Veränderns oder Entfernens von fremden Daten während einer Dateiübermittlung oder während einer Speicherung auf einem Datenträger sowie Beschränkung der Datenübermittlung auf legitime Adressaten,
- *Eingabekontrolle* hinsichtlich der Protokollierung, ob und von wem Daten eingegeben, verändert oder entfernt wurden,
- *Auftragskontrolle* bei der Verarbeitung von Daten im Wege einer Auftragsdatenverarbeitung,
- *Verfügbarkeitskontrolle* hinsichtlich des Schutzes von Daten gegen zufällige Zerstörung und gegen Verlust,
- sowie zum *Trennungsprinzip* hinsichtlich der Nichtzusammenführbarkeit von zu unterschiedlichen Zwecken erhobenen Daten.

Auch hinsichtlich automatisierter Systeme sind diese IT-Sicherheitszielsetzungen des BDSG von Relevanz, was an dem Beispiel „automatisierte Dienstleistungsdrohne zur Paketzustellung“ verdeutlicht werden soll. Datenschutzrechtliche Relevanz entfaltet der Einsatz automatisierter Drohnen deswegen, da diese zur Koordinierung und zur Orientierung im Raum sowie zum Schutz von Personen, Gegenständen und anderen Luftfahrzeugen stets ihre Umgebung scannen, also mittels Kameratechnik optisch-elektronisch erfassen, müssen. Hierbei werden mitunter auch personenbezogene oder zumindest -beziehbare Daten erhoben und verarbeitet, sodass die datenschutzrechtlichen Bestimmungen des BDSG und daher auch die sicherheitsrechtlichen Bestimmungen des § 9 BDSG i.V.m. der Anlage zum BDSG einschlägig sind. Vgl. zu der datenschutzrechtlichen Perspektive bereits das Kapitel 2.3.

- *Zutrittskontrolle:* Paketdrohnen bedürfen einer zentralen Kommandoeinheit am Boden, die den Drohnen ihre Lieferaufträge übermittelt, diese überwacht und ggf. steuernd eingreift. Dazu hat der Betreiber eine Steuer-, Server- und Kommunikationsanlage zu betreiben. Im Rahmen der Zutrittskontrolle hat dieser dabei sicherzustellen, dass diese zentralen Anlagen hinreichend vor unberechtigtem Betreten gesichert sind (etwa: bauliche und räumliche Abschottung vor unberechtigten Dritten).
- *Zugangskontrolle:* Diese Serveranlagen sind mit Hilfe eines sicheren Benutzermanagements vor einer unberechtigten Nutzung durch Dritte zu schützen. Zudem sind auch die im Einsatz befindlichen Paketdrohnen dahingehend zu schützen, dass ein unberechtigter Dritter die Kommunikationsverbindung zu der Serveranlage nicht nutzen kann, um selbst Zugang zu der Drohnenfirmware zu erhalten (etwa: sicheres Identitätsmanagement und Authentifizierung).
- *Zugriffskontrolle:* Es ist zudem sicherzustellen, dass eine an sich zur Nutzung des Systems berechtigte Person nur auf die ihr zugewiesenen Dateien und Operationen Zugriff hat. Insofern ist ein Rechte- und Rollenmanagement einzurichten, das einen Exzess (eine Überschreitung der eingeräumten Befugnisse) des Nutzers verhindert.
- *Weitergabekontrolle:* Die Datenverbindung des Servers zu den Drohnen ist sicher auszugestalten. Insbesondere ist diese gegen fremdes Auslesen zu schützen (etwa: Verschlüsselung und Signierung der Kommunikationsverbindung).
- *Eingabekontrolle:* Die Kommunikation zwischen Server und Drohne ist zu protokollieren. Zudem sind alle bei einer Paketzustellung anfallenden Metadaten zu dokumentieren.
- *Auftragskontrolle:* Lässt der Paketdienst personenbezogene Daten im Auftrag von einem externen Dienstleister verarbeiten, ist hierbei sicherzustellen, dass diese ausschließlich entsprechend den Weisungen des Paketdienstes verarbeitet werden.
- *Verfügbarkeitskontrolle:* Der Paketdienst hat seine Serversysteme gegen zufälligen Datenverlust zu schützen. Dies wird unter anderem durch die Einrichtung geeigneter und redundanter Sicherungsmaßnahmen gewährleistet. Zudem sind die Serveranlagen gegen Schäden durch Naturgewalten (Wasserschaden, Blitzschlag, u.a.) entsprechend abzusichern.
- *Trennungsprinzip:* Die Versandinformationen (Inhalt der Bestellung, Datum, Adresse, Metadaten der Zustellung, etc.) der verschiedenen Kunden sind voneinander getrennt zu verarbeiten. Zudem sind diese Versandinformationen von weiteren Metadaten getrennt zu speichern.

2.5.2 EU-DSGVO

Hinsichtlich der Datensicherheit der erhobenen und auf den automatisierten Systemen gespeicherten Daten sind zukünftig auch die Bestimmungen der *EU-DSGVO* zu beach-

ten. Im Anwendungsbereich der EU-DSGVO genießt diese gegenüber dem BDSG zukünftig Anwendungsvorrang.

So gibt bereits Art. 5 Abs. 1 lit. f EU-DSGVO den Grundsatz vor, dass die Sicherheit („Integrität und Vertraulichkeit“) personenbezogener Daten hinreichend gewährleistet werden muss und diese insbesondere vor einer unbefugten oder unrechtmäßigen Verarbeitung, vor unbeabsichtigten Verlust, vor unbeabsichtigter Zerstörung und vor unbeabsichtigter Beschädigung durch geeignete technische und organisatorische Maßnahmen geschützt werden müssen.

Dieser Grundsatz wird von Art. 32 EU-DSGVO erneut aufgegriffen, der unter anderem bestimmt, dass „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen […] der Verantwortliche […] geeignete technische und organisatorische Maßnahmen [treffen muss], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“.

Im Vergleich zu der Anlage zu § 9 BDSG enthält Art. 32 Abs. 1 EU-DSGVO zwar keine wortlautgleichen IT-Sicherheitszielbestimmungen. Doch bestimmt auch Art. 32 Abs. 1 EU-DSGVO weiter, dass von den zu treffenden Maßnahmen auch die „Pseudonymisierung und Verschlüsselung personenbezogener Daten“ (a), „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen“ (b), „die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen“ (c) sowie „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ (d), eingeschlossen seien. Hinsichtlich der Datensicherheit führen die Bestimmungen des Art. 32 Abs. 1 EU-DSGVO daher im Ergebnis zu einem mit der Anlage zu § 9 BDSG vergleichbaren Schutzniveau.

2.5.3 IT-Sicherheitsgesetz

Die Betreiber kritischer Infrastrukturen haben künftig gem. § 8a Abs. 1 BSIG „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, *Integrität, Authentizität und Vertraulichkeit* ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind“. Das IT-Sicherheitsgesetz bezweckt damit einerseits die Gewährleistung von Funktionssicherheit (Verfügbarkeit), andererseits aber auch die Sicherstellung von Informationssicherheit (Integrität, Authentizität und Vertraulichkeit).

Zwar ist das IT-Sicherheitsgesetz zunächst nur für die Betreiber kritischer Infrastrukturen relevant. Nicht auszuschließen ist aber, dass auch diese zur Erledigung ihrer Aufgaben automatisierte Systeme einsetzen. In diesem Fall finden die Bestimmungen des

IT-Sicherheitsgesetzes auch auf die technische Ausgestaltung der automatisierten Systeme Anwendung.

2.5.4 NIS-Richtlinie

Die europäische NIS-Richtlinie bezweckt die Erhöhung der Sicherheit von Netz- und Informationssystemen in den EU-Mitgliedstaaten. Hält man sich vor Augen, dass Automatisierung derzeit stets auch mit Vernetzung einhergeht und in den USA gar eine Vernetzungspflicht von automatisierten Kfz diskutiert wird,[37] wird deutlich, dass die NIS-Richtlinie gerade auch auf die Entwickler und Betreiber automatisierter Systeme Anwendung finden kann. Die NIS-RL wurde bereits am 6.7.2016 vom europäischen Gesetzgeber verabschiedet und ist daraufhin am 8.7.2016 in Kraft getreten. Als europäische Richtlinie entfaltet die NIS-RL aber keine unmittelbare Rechtswirkung, sondern muss bis zum 9.5.2018 noch in nationales Recht umgesetzt werden.

Im Rahmen der NIS-RL sollen dabei neue Sicherheitsanforderungen und Meldepflichten für die Betreiber sog. „wesentlicher Dienste“ und für die Anbieter „digitaler Dienste“ definiert werden. Was ein „wesentlicher Dienst“ im Sinne der Richtlinie ist, soll nach Art. 5 Abs. 1 der NIS-RL von den Mitgliedstaaten bis zum 9.11.2018 ermittelt werden. Nach der Formulierung des Art. 5 Abs. 2 der NIS-RL („Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten“, „erhebliche Störungen“) ist aber bereits erkennbar, dass hier eine Parallele zu dem Begriff der „Betreiber kritischer Infrastrukturen“ im Sinne des IT-Sicherheitsgesetzes bestehen wird.

Nicht ausgeschlossen ist daher, dass auch spezifische Entwickler und Anwender von automatisierten Systemen solche „wesentliche Dienste“ oder „digitale Dienste“ (etwa automatisierte Softwareprodukte) bereitstellen oder nutzen und daher auch bei der Ausgestaltung dieser automatisierten Systeme auf die Erfordernisse der NIS-RL, bzw. auf das ergehende nationale Umsetzungsgesetz, zu achten ist.

2.5.5 Handlungsempfehlungen des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht regelmäßig eigene *Handlungsempfehlungen* und *Maßnahmenkataloge*, die der Anwender zur Umsetzung seiner IT-Sicherheitsverpflichtungen (unter anderem aus § 9 BDSG) zu Rate ziehen kann. Auch wenn nach § 9 BDSG der Betreiber einer Datenverarbeitungsanlage verpflichtet ist, entsprechende Sicherheitsvorkehrungen zu treffen, so stellen die Handlungsempfehlungen des BSI dennoch nur freiwillige Standards mit richtungsweisendem Charakter dar. Insofern steht dem Betreiber offen, seine Verpflichtungen

[37] http://www.golem.de/news/einbaupflicht-gefordert-usa-setzen-beim-vernetzten-fahren-auf-wlan-1612-125097.html (abgerufen am 21.12.2016).

auch durch andere Standards und Maßnahmenkataloge zu erfüllen. Im Rahmen der Handlungsempfehlungen des BSI sind dann insbesondere die *BSI IT-Grundschutz-Kataloge* relevant, die grundlegend in Gefährdungs- und in Maßnahmenkataloge unterteilt werden.

Die Gefährdungskataloge enthalten insofern eine Aufzählung der denkbaren Gefährdungslagen beim Einsatz von IT. Diese betreffen neben technischem Versagen auch organisatorische Mängel, menschliche Fehlhandlungen oder höhere Gewalt. Die Maßnahmenkataloge enthalten sodann konkrete Handlungsempfehlungen, um diesen Gefährdungslagen bestmöglich zu begegnen. Auch diese betreffen insofern nicht nur technische und infrastrukturelle, sondern auch organisatorische und personelle Gegenmaßnahmen.

Aufgrund des modularen Aufbaus der IT-Grundschutzkataloge sind diese grundsätzlich offen ausgestaltet und nicht auf spezifische Systeme beschränkt. Denn anstatt spezifische Gesamtsysteme darzustellen, enthalten die IT-Grundschutzkataloge vielmehr nur Darstellungen einzelner, in einem Gesamtsystem verbauter IT-Komponenten. Dies führt dazu, dass der Anwender sein zu prüfendes Gesamtsystem zunächst in seine Einzelkomponenten auftrennen und entkoppeln muss und dann im Rahmen der komponentenbezogenen Bestimmungen der IT-Grundschutzkataloge sein System modelliert und analysiert. Welche Bestimmungen der IT-Grundschutzkataloge daher für ein automatisiertes System relevant sind, ist erneut abhängig von der Art und der Ausgestaltung des Systems.

Beispiel: *In einer Produktionshalle sollen intelligente Roboter miteinander kommunizieren. Der einsetzende Unternehmer überlegt, ob er bei der Verwendung von Wireless LAN (WLAN) spezifische IT-Sicherheitsstandards zu beachten hat. In dem IT-Grundschutzkatalog-Baustein B4.6 befinden sich Ausführungen zum sicheren Einsatz von WLAN. Dieser Baustein untergliedert sich in Ausführungen zur Gefährdungslage (durch höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen, vorsätzliche Handlungen) sowie in konkrete Maßnahmenempfehlungen zur Beseitigung oder Minimierung dieser Gefahren. Aufgrund dieser Maßnahmenempfehlungen wird der Unternehmer sein WLAN etwa dem Stand der Technik entsprechend verschlüsseln und auch alle eingesetzten Access Points und Router dementsprechend absichern. Weiterhin wird er einen Notfallplan mit Verhaltensregeln bei zukünftigen WLAN-Sicherheitsvorfällen bereithalten.*

2.5.6 ISO/IEC 27000-Standards

Auch die sog. ISO/IEC 27000-Familie, die von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) herausgegeben wird, stellt eine Reihe an IT-Sicherheitsstandards und damit ebenfalls freiwillige Handlungsempfehlungen für die Betreiber von IT dar. Auch im Rahmen der ISO/IEC 27000-Reihe existieren (bislang) keine automatisierungsspezifischen Richtlinien, sodass je nach verwendeten Einzelkomponenten ein Querschnitt aus allen ISO/IEC 27000-Dokumenten in Betracht kommt.

2.5.7 Weitere IT-Sicherheitsstandards

Die bereits oben im Rahmen der Funktionssicherheit genannten ISO / IEC / EN / DIN-Normen (vgl. hierzu Kapitel 2.4.2) enthalten stellenweise auch Vorschriften zur Informationssicherheit von IT-Systemen und sind in diesem Kontext gleichwohl heranzuziehen. Dies betrifft beispielsweise die ISO/IEC 15408, die neben funktionalen Sicherheitsanforderungen für IT-Produkte und IT-Systeme (Teil 2) auch Anforderungen an die Vertrauenswürdigkeit dieser Systeme beinhaltet (Teil 3).

3 Haftung

Haftungskonstellationen und Haftungsnormen bei automatisierten Systemen

3.1 Haftungsszenarien

Ebenso vielfältig wie die Einsatzszenarien von automatisierten Systemen – man denke hierbei nur an die unterschiedlichen Ausgestaltungen (etwa Industrieroboter, Dienstleistungsroboter, automatisierte Straßenfahrzeuge, automatisierte Drohnen, etc.) und an die grenzenlosen Einsatzgebiete (etwa in der Industrie, im Transportwesen, im Pflege- und Gesundheitswesen, durch den Staat, im Haushalt, etc.) – sind auch die denkbaren Gefährdungsszenarien, die von solchen Systemen ausgehen können. Denn jede technische Entwicklung bringt naturgemäß auch neuartige Gefährdungspotentiale mit sich, die gerade am Anfang einer neuen Produktgattung einer stetigen Produktverbesserung und Weiterentwicklung bedürfen. Nicht alle technischen Fehlerquellen lassen sich insofern bereits in der Entwicklungsphase „am Reißbrett“ identifizieren und eliminieren. Oftmals bedarf es hierzu vielmehr einer Erprobung im tatsächlichen Einsatz, was jedoch stets die Gefahr der Verletzung einer Person oder der Beschädigung einer Sache mit sich bringt. Doch nicht nur technische Fehlfunktionen können Auslöser von Personenverletzungen oder Sachbeschädigungen sein – auch eine fehlerhafte Bedienung oder eine fehlerhafte Wartung des Systems kommt hierbei in Betracht.

Setzt ein Dienstleister oder ein Unternehmen ein automatisiertes System, etwa einen automatisierten Industrieroboter, ein, oder aber stellt dieser selbst solche automatisierten Systeme her, stellt sich insofern stets die Frage, welche Haftungsszenarien hierbei in Betracht kommen, wenn durch die Verwendung des Systems Sachen beschädigt oder Personen verletzt werden. Zu klären ist hierbei zunächst, welche Fehlerquellen überhaupt zu einer fehlerhaften technischen Reaktion führen können und wer Betroffener eines solchen technischen Fehlverhaltens sein kann (wer also hierdurch verletzt werden kann oder wessen Sachen hierdurch beschädigt werden können). Anschließend stellt sich stets die wichtige Frage, welche Haftungsadressaten bei etwaigen Schadensersatzforderungen herangezogen werden können.

3.1.1 Fehlerquellen bei automatisierten Systemen

Als Fehlerquellen eines automatisierten Systems kommen zunächst eine *fehlerhafte Softwareprogrammierung* oder aber ein *Hardwareversagen* in Betracht. Automatisierte Systeme sind insbesondere auf die Erhebung und Verarbeitung zahlreicher Sensordaten angewiesen, um eine exakte und fehlerfreie Programmausführung zu gewährleisten. Durch den hardwareseitigen Ausfall von Sensoren bzw. durch Abweichungen in der Messgenauigkeit können daher ebenso technische Fehlreaktionen ausgelöst werden wie durch eine softwareseitige Störung bei der Datenverarbeitung, wenn die korrekt erhobenen Daten also fehlerhaft ausgewertet werden.

Neben diesen Fehlern in der Hard- oder Software kann ein automatisiertes System weiterhin stets nur *im Rahmen der vorgegebenen Programmierung* funktionieren. Werden bestimmte Verhaltensweisen und Algorithmen im Rahmen der Entwicklung falsch vorgegeben, kann dies insofern zu objektiv unerwünschten Reaktionen führen, die aber weder auf einem Software- noch auf einem Hardwareversagen beruhen, sondern lediglich Folge eines inadäquat ausgestalteten Systems sind. Diese adäquate Systemausgestaltung wird insbesondere auch bei fortgeschrittenen künstlich intelligenten und selbstlernenden Systemen künftig eine besondere Rolle spielen. Zwar sind selbstlernende Systeme generell in der Lage, eigene Verhaltensweisen anzulernen, was generell eine weitere Fehlerquelle automatisierter Systeme darstellen kann. Gleichwohl gilt hier die vorgegebene Programmierung aber weiterhin als äußerster Begrenzungsrahmen der „Lernfreiheit“ des Systems.

Doch selbst wenn sowohl die Hard- und Software ordnungsgemäß funktioniert und dem System weiterhin auch eine adäquate Technikgestaltung zugrunde liegt, kann es dann zu Funktionsstörungen kommen, wenn ein *unberechtigter Dritter Zugriff auf das System* erhält und dieses insofern „kapert“ (sog. „Hijacking“). Im Rahmen der Realisierung von IT-Sicherheit sind daher zum einen die auf dem System gespeicherten personenbezogenen Daten (Teilbereich der Informationssicherheit), zum anderen aber auch das System selbst vor einer unautorisierten Kontrollübernahme (Teilbereich der Funktionssicherheit) zu schützen.

Ein automatisiertes System, etwa ein automatisierter Industrieroboter, bedarf weiterhin stets einer *fachmännischen Installation am Einsatzort sowie einer ständigen Wartung und Aktualisierung* der Betriebssoftware. Durch eine mangelhafte Wartung oder durch den Betrieb einer veralteten Firmware können insofern zahlreiche Funktionsstörungen ausgelöst werden, welche wiederum zu der Verletzung von Personen oder der Beschädigung von Sachen führen können.

Zuletzt stellt der Endnutzer stets auch selbst eine Fehlerquelle dar, da ein automatisiertes System *lediglich innerhalb seiner Leistungsgrenzen und nur in der vorgeschriebenen ordnungsgemäßen Art und Weis*e eingesetzt werden darf. Hierfür verantwortlich kann bei der Verwendung eines automatisierten Industrieroboters etwa der für das System zuständige Angestellte sein, der das System stets fachmännisch zu bedienen hat und sich im Wege von Schulungen auch regelmäßig über technische Neuerungen weiterbilden muss. Gerade bei der privaten Verwendung von automatisierten Dienstleistungsrobotern im Zuhause des Anwenders tragen zudem auch die Käufer und Inhaber des Systems die Pflicht, ihr automatisiertes System nur ordnungsgemäß nach Anleitung oder Instruktion einzusetzen und zu bedienen sowie fachmännisch zu warten und zu aktualisieren.

3.1.2 Betroffene bei Funktionsstörungen automatisierter Systeme

Kommt es zu einer Funktionsstörung oder einem sonstigen Fehlverhalten eines automatisierten Systems, ist zuvorderst der unmittelbare Nutzer und Anwender gefährdet, also derjenige, der sich in der räumlichen unmittelbaren Nähe des Systems befindet.

Dies kann bei dem Einsatz eines automatisierten Industrieroboters etwa der sich im Umfeld befindliche Arbeitnehmer sein, bei einem Krankenpflegeroboter der zu behandelnde Patient oder aber die bedienende Pflegekraft.

Neben diesen unmittelbar betroffenen Personen kann auch das einsetzende Unternehmen Nachteile durch eine Funktionsstörung des automatisierten Systems tragen. Denn wird das fehlerhafte System selbst oder andere Maschinen oder Sachen des Unternehmens beschädigt oder muss das fehlerhafte System zur zukünftigen Korrektur des Fehlers zeitaufwendig aktualisiert oder repariert werden, kann hierdurch ein massiver Produktionsrückstau entstehen. Dies wiederum kann zu Produktionsverzögerungen, zu Auftragsstornierungen oder gar zu Schadensersatzforderungen und mithin zu Umsatzeinbußen führen.

Hält man sich den oben im Datenschutzteil besprochenen Fall (vgl. Kapitel 2.3.4) des Einsatzes einer Industriedrohne vor Augen, die zur Wahrnehmung ihrer Aufgaben auch öffentliches Terrain überfliegen muss, wird weiterhin schnell deutlich, dass auch unbeteiligte Passanten verletzt oder deren Sachen beschädigt werden können, wenn die eingesetzte Drohne abstürzt oder sonst mit einem Passanten kollidiert. Neben einer solchen körperlichen oder gesundheitlichen Verletzung des Passanten oder der Beschädigung einer seiner Sachen kommt hierbei auch eine Verletzung des Rechts auf informationelle Selbstbestimmung und des Persönlichkeitsrechts in Betracht, wenn personenbezogene oder –beziehbare Daten über diese Person rechtswidrig erhoben, verarbeitet oder genutzt werden.

3.1.3 Haftungsadressaten bei Funktionsstörungen automatisierter Systeme

Wird bei dem Einsatz eines automatisierten Systems eine Person verletzt, eine Sache beschädigt oder ein sonstiges Recht (etwa das Datenschutzrecht) beeinträchtigt, kommen mehrere Haftungsadressaten in Betracht. Ausgehend von der jeweiligen Fehlerquelle (vgl. oben Kapitel 3.1.1) wird hierbei regelmäßig zunächst derjenige herangezogen werden, der den Fehler zu vertreten hat. Im Wege der im deutschen Recht stellenweise vorzufindenden Gefährdungshaftung kann dieser Grundsatz jedoch dort durchbrochen sein, wo der Halter eines Systems (etwa bei automatisierten Fahrzeugen) auch ohne eigenes Verschulden haftet.

Je nach Art und Weise sowie Einsatzort des automatisierten Systems kommen als Haftungsadressaten grundsätzlich in Betracht: 1) der Hersteller und Entwickler des automatisierten Systems, 2) bei der Entwicklung ggf. beteiligte weitere Dritte (etwa Zulieferer für die Firmware oder einzelner technischer Komponenten, etc.), 3) ggf. Zwischenhändler, die das System an den Endnutzer vertreiben, 4) das einsetzende Unternehmen, 5) bei Industrie- und Dienstleistungsrobotern der mit dem System betraute Arbeitnehmer, 6) bei Dienstleistungsrobotern für den Privatgebrauch der Endnutzer, 7) bei einer auf einen unbefugten Eingriff oder Angriff durch Dritte (etwa durch Hacker) zurückzuführenden Fehlreaktion weiterhin auch dieser Dritte.

Weiterhin kommt auch eine Haftung des Netzbetreibers bei einem Netzausfall in Betracht, da automatisierte und vernetzte Systeme hochgradig von einem stabilen Datenaustausch untereinander abhängig sind. Im Falle von in der Öffentlichkeit agierenden Systemen wird dies zukünftig zuvorderst über das Mobilfunknetz (insbesondere über LTE (4G-Standard) und über den geplanten 5G-Standard) geschehen. Eine solche Haftung wird sich insbesondere aus den zwischen dem Telekommunikationsanbieter und dem Betreiber des automatisierten Systems geschlossenen Verträgen ergeben. Meist behält sich der Telekommunikationsanbieter hierbei aber einen gewissen Prozentanteil an legitimen Ausfallzeiten vor, für die dann kein Schadensersatz verlangt werden kann.

3.2 Maßstäbe und Rechtgrundlagen der Haftung

Eine Haftung kann sich im deutschen Recht aus allgemeinen Vorschriften (etwa aus dem BGB), oder aber aus Spezialgesetzen (etwa aus dem StVG, dem LuftVG oder dem ProdHaftG) ergeben. Weiter kann sich eine Haftung einerseits aus einer vertraglichen Beziehung des Beschädigten zum Schädiger ergeben, also etwa dann, wenn eine vertragliche Pflicht gebrochen wurde. Andererseits kann sich eine Haftung aber auch außervertraglich, etwa aus dem Deliktsrecht, ergeben. Die einzelnen Haftungsnormen unterscheiden sich weiterhin auch nach ihrem Verschuldensmaßstab: abzugrenzen ist hierbei die Verschuldenshaftung zu der Haftung aus vermutetem Verschulden zu der Gefährdungshaftung.

3.2.1 Vertragliche Haftung

Schließen Parteien wirksam einen Vertrag, so erhält der Gläubiger aus dem vertraglichen Schuldverhältnis einen Anspruch gegen den Schuldner, also das Recht, von diesem ein Tun oder Unterlassen zu fordern (vgl. § 194 Abs. 1 BGB). Welches Tun oder Unterlassen hierbei konkret gefordert werden kann, ist dabei abhängig von dem jeweiligen Vertragsverhältnis. Bei einem Kaufvertrag wird der Verkäufer einer Sache nach § 433 Abs. 1 BGB etwa verpflichtet, dem Käufer die Sache zu übergeben und das Eigentum an der Sache – frei von Sach- und Rechtsmängeln – zu verschaffen. Der Käufer ist nach § 433 Abs. 2 BGB dagegen verpflichtet, dem Verkäufer den vereinbarten Kaufpreis zu zahlen und die Sache abzunehmen. Beim Werkvertrag dagegen wird der Unternehmer nach § 631 Abs. 1 BGB zur Herstellung des versprochenen Werkes und der Besteller zur Entrichtung der vereinbarten Vergütung verpflichtet. Auch hierbei hat der Unternehmer dem Besteller gem. § 633 Abs. 1 BGB das Werk frei von Sach- und Rechtsmängeln zu verschaffen. Weiterhin relevant ist auch der Dienstleistungsvertrag nach §§ 611 ff. BGB.

Aus dem Grundsatz der Privatautonomie (aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG) folgt, dass die Parteien in ihrer Vertragsgestaltung grundsätzlich frei sind. Diese können daher also nicht nur Verträge schließen, deren Typus ausdrücklich gesetzlich geregelt ist (etwa einen Kaufvertrag oder einen Werkvertrag), sondern grundsätzlich jede Art von Vertragsverhältnis, das den Schuldner und den Gläubiger dann an eine Vielzahl an

unterschiedliche Pflichten bindet. In diesem Kontext relevant sind insbesondere auch sog. gemischte Verträge, bei denen umfassende Rechte und Pflichten beider Vertragsparteien vereinbart werden, die unterschiedliche Vertragsarten betreffen. So werden in dem Verhältnis Anbieter (Hersteller oder Verkäufer des automatisierten Systems) und Anwender (der das System einsetzende Unternehmer oder die das System erwerbende Privatperson) etwa oftmals Kombinationen aus Kaufverträgen/Werk(lieferungs)verträgen (bspw. die Anschaffung und Herstellung des Systems selbst) und Dienstleistungsverträgen (bspw. die ständige Wartung und Aktualisierung des Systems bzw. die Versorgung mit „Patches“, also Updatepaketen mit Fehlerverbesserungen) in einem übergreifenden „Roboterbeschaffungs- und Roboterwartungsvertrag“ vereinbart werden.

Neben herkömmlicher Patches (Fehlerkorrekturen) und in regelmäßigen Intervallen ergehender Updates (Produktaktualisierungen), werden beim Einsatz automatisierter Systeme zukünftig auch sog. Produktbeobachtungspflichten eine besondere Rolle spielen. Denn die Komplexität der Umgebungen, in denen automatisierte Systeme eingesetzt werden sollen, erschwert zunehmend eine abschließende funktionssichere Systementwicklung „am Reißbrett“. Vielmehr werden automatisierte Systeme zukünftig in der Produktivumgebung einzusetzen, zu beobachten und permanent mit Produktverbesserungen zu aktualisieren sein, wenn unvorhergesehene Umgebungseinflüsse Änderungen im System erforderlich machen.

Wird eine vertragliche Pflicht verletzt, kann dies der gegnerischen Partei einen Anspruch auf Schadensersatz aus den §§ 280 ff. BGB vermitteln, wenn diese Pflichtverletzung durch den Schuldner oder durch einen diesem zurechenbaren Dritten (vgl. § 278 BGB) vorsätzlich oder fahrlässig (sog. „Vertretenmüssen“, vgl. § 276 Abs. 1 S. 1 BGB) begangen wurde. Der konkrete Umfang der Schadensersatzpflicht richtet sich dabei nach den §§ 249 ff. BGB, wonach beispielsweise Behandlungskosten zu erstatten sowie beschädigte Sachen zu reparieren und zu ersetzen sind.

3.2.2 Außervertragliche Haftung

Kapitelübersicht

Neben der vertraglichen Haftung kommt auch eine außervertragliche Haftung in Betracht. Diese bedarf grundsätzlich keines vorherigen Vertragsverhältnisses zwischen dem Schädiger und dem Geschädigten und kann daher als eigenständige Anspruchsgrundlage eines unbeteiligten Dritten oder aber neben einem weiterhin bestehenden vertraglichen Anspruch bestehen.

3.2.2.1 Verschuldenshaftung

Im Deliktsrecht haftet grundsätzlich nur derjenige, der eine Verletzungshandlung vorsätzlich oder fahrlässig (sog. Verschulden) begangen hat (vgl. § 823 Abs. 1 BGB). Das Vorliegen eines Verschuldens stellt demnach grundsätzlich eine notwendige Tatbestandsvoraussetzung dar, die grundsätzlich die klagende Partei positiv beweisen muss. Gelingt der Nachweis nicht, so ist der Anspruch nicht durchsetzbar. Die zentrale Deliktshaftungsnorm des § 823 Abs. 1 BGB stellt etwa eine solche Verschuldenshaftung dar.

3.2.2.2 Haftung aus vermutetem Verschulden

Im Gegensatz dazu wird ein Verschulden bei manchen Haftungstatbeständen zulasten des Schädigers widerlegbar vermutet. Hierbei muss also nicht die klagende Partei das Vorliegen eines Verschuldens beweisen, sondern vielmehr kann sich der Beklagte lediglich exkulpieren, also den Gegenbeweis erbringen, um einer Haftung zu entgehen. Eine solche Haftung aus vermutetem Verschulden liegt etwa im Rahmen der Fahrzeugführerhaftung nach § 18 Abs. 1 StVG vor.

3.2.2.3 Gefährdungshaftung

Als Ausnahme von dem Grundsatz, dass nur derjenige Verursacher für einen Schaden haften muss, der diesen auch verschuldet hat, sieht das deutsche Recht stellenweise aber auch eine sog. Gefährdungshaftung vor. Hiernach muss auch für solche Schäden gehaftet werden, die von dem in Anspruch genommenen nicht vorsätzlich oder fahrlässig herbeigeführt wurden. Eine solche Gefährdungshaftung wird regelmäßig darin begründet und gerechtfertigt, dass von dem Anspruchsgegner eine Gefahr in die Welt gesetzt wurde, für die dieser unabhängig eines eigenen Verschuldens einzustehen hat. So sind bestimmte Verhaltensweisen zwar abstrakt gefährlich (etwa das Fahren eines Autos), aber dennoch erlaubt, da ihre soziale Nützlichkeit überwiegt. Der Halter eines Fahrzeugs handelt nicht rechtswidrig, nur weil er ein Auto hat, auch wenn er weiß, dass von einem Auto im Straßenverkehr gewisse Gefahren ausgehen. Dennoch hat der Fahrzeughalter verschuldensunabhängig diejenigen Schäden zu ersetzen, die in den Risikobereich des Fahrzeugs fallen, vgl. § 7 StVG. Auch der Hersteller eines Produkts ist unter Umständen verschuldensunabhängig zum Schadensersatz verpflichtet, da das bloße Inverkehrbringen des Produkts schon eine Gefahr darstellt, vgl. § 1 ProdHaftG. Eine solche Gefährdungshaftung enthält darüber hinaus auch § 8 Abs. 1 BDSG, wonach eine *öffentliche Stelle* „unabhängig von einem Verschulden“ dem von

einer unzulässigen automatisierten Datenverarbeitung Betroffenen zum Schadensersatz verpflichtet ist.

3.2.2.4 Konkrete außervertragliche Haftungsanspruchsgrundlagen

Im Folgenden sollen die im Kontext von automatisierten Systemen in Betracht kommenden außervertraglichen Haftungsanspruchsgrundlagen überblicksmäßig (und nicht abschließend) aufgezeigt werden.

3.2.2.4.1 § 823 Abs. 1 BGB

§ 823 Abs. 1 BGB gilt als zentraler Haftungstatbestand, wenn jemand vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, das Eigentum oder ein sonstiges absolutes Recht eines anderen widerrechtlich verletzt.

Im Rahmen des Einsatzes automatisierter Systeme kommt diese Anspruchsgrundlage insbesondere dann in Betracht, wenn ein Arbeitnehmer, ein Passant oder ein anderer Beteiligter verletzt wird oder dessen Sachen beschädigt werden. Haftungsadressat ist dabei derjenige, der die Pflichtverletzung und den Schaden kausal und verschuldet herbeigeführt hat. Dies kann zunächst der bedienende Arbeitnehmer sein, wenn dieser aufgrund eines eigenen Fehlverhaltens eine Fehlfunktion des Systems herbeiführt. Weiter kann aber auch das Unternehmen selbst aufgrund organisatorischen Fehlverhaltens notwendige Wartungen versäumt oder das System falsch installiert und hierdurch die Verletzung von Rechten Dritter verschuldet haben. Schließlich kann eine Rechtsverletzung auch auf einen Produktfehler zurückzuführen sein, für den der Hersteller und Entwickler einzustehen hat.

3.2.2.4.2 § 823 Abs. 2 BGB

Nach § 823 Abs. 2 BGB trifft eine Verpflichtung zum Schadensersatz auch denjenigen, der gegen ein sog. Schutzgesetz verstößt. Ein solches Schutzgesetz können etwa eine Strafnorm des StGB, aber auch diverse andere Rechtsnormen sein, die nicht nur den Schutz der Allgemeinheit sondern gerade auch eines Einzelnen bezwecken (sog. Individualschutz).

Im Kontext des Einsatzes von automatisierten Systemen kommt als ein solches Schutzgesetz insbesondere auch das Produktsicherheitsgesetz in Betracht, das in § 3 ProdSG bestimmt, dass kein unsicheres Produkt auf den Markt gelangen darf.

Aber etwa auch Normen aus dem Medizinproduktegesetz sowie aus der MPBetreibV können solche Schutzgesetze sein, die bei Zuwiderhandlung Schadensersatzansprüche nach dem § 823 Abs. 2 BGB auslösen können.

In Betracht kommt hierbei weiterhin eine Verletzung des Luftverkehrsrechts bei der Nutzung von Drohnen, die über § 823 Abs. 2 BGB (und damit neben § 33 LuftVG) ebenfalls zu Schadensersatzansprüchen führen kann.

3.2.2.4.3 § 1 ProdHaftG

Nach § 1 Abs. 1 ProdHaftG haftet der Hersteller eines Produkts, wenn durch einen Produktfehler ein Mensch getötet, sein Körper oder seine Gesundheit verletzt oder eine fremde Sache beschädigt wird. Der Geschädigte hat insofern nachzuweisen, dass ein fehlerhaftes Produkt vorlag und seine Schädigung auf diesen Fehler zurückzuführen ist, § 1 Abs. 4 ProdHaftG. Auf ein Verschulden kommt es anders als i.R.d. Produzentenhaftung gem. § 823 Abs. 1 BGB hier aber nicht an (sog. Gefährdungshaftung, vgl. oben Kapitel 3.2.2.3).

Gerade beim Einsatz von automatisierten Systemen könnte zukünftig eine nicht zu unterschätzende Haftungsverschiebung hin zum Hersteller und Entwickler des Produkts stattfinden. Im Kontext des automatisierten Fahrens etwa könnte dies zu einer Haftungsverlagerung vom Fahrzeughalter und –führer hin zum Automobilhersteller führen. Denn während beim manuell gesteuerten Kfz der Hersteller nur für sog. Konstruktions- oder Fabrikationsfehler einzustehen hatte, könnte dieser nun auch für konkrete Fahrfehler des automatisierten Kfz aufkommen müssen, wenn die automatisierten Handlungen und Reaktionen des Fahrzeugs bereits ab Werk vorgegeben werden und diese die Ursache eines Unfalls waren. Hierbei besteht insbesondere auch die Gefahr, dass sich der Fahrzeugführer bei einem Unfall künftig stets auf ein Versagen des Kfz beruft, auch wenn dieser das Fahrzeug selbst gesteuert hat. Dies erfordert insbesondere technische Lösungen, die den Kausalitätsverlauf eines Unfalls protokollieren und rechtssicher nachweisen können. Einen ersten Ansatz hierzu verfolgt der Gesetzgeber bereits in dem neuen § 63a StVG, der vorsieht, dass die Steuerungsübernahme durch den Fahrzeugführer oder durch das automatisierte System von dem Fahrzeug protokolliert wird.

3.2.2.4.4 § 7 BDSG und Art. 82 EU-DSGVO

§ 7 BDSG enthält eine Haftungsanspruchsnorm, wenn eine verantwortliche Stelle dem Betroffenen durch eine nach dem BDSG oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zufügt. Nach Satz 2 dieser Vorschrift kann die Haftung dann entfallen, wenn die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat. Wer dabei verantwortliche Stelle im Kontext der Vorschrift ist, bestimmt sich danach, welche Person oder Stelle die personenbezogenen Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (vgl. § 3 Abs. 7 BDSG).

Gerade automatisierte Systeme sind permanent auf die Erhebung und Verarbeitung zahlreicher Sensordaten angewiesen. Wie bereits gezeigt wurde, dient eine solche

umfassende Datenerhebung gar der Verbesserung der Funktionssicherheit, da nur mittels dieser Sensordaten andere Personen im Umfeld erkannt und geschützt werden können. Dennoch muss jene Datenerhebung und –verarbeitung stets mit dem BDSG konform sein. Ist sie dies nicht, kommt den Betroffenen ein Schadensersatzanspruch aus § 7 BDSG zu.

Mit Inkrafttreten der Europäischen Datenschutzgrundverordnung ab dem Jahr 2018 wird an Stelle der haftungsrechtlichen Bestimmungen des BDSG Art. 82 EU-DSGVO zu beachten sein. Auch hiernach hat „jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, [...] Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter“ (Art. 82 Abs. 1 EU-DSGVO). Gem. Art. 82 Abs. 3 EU-DSGVO besteht aber wiederum die Möglichkeit des Verantwortlichen oder des Auftragsverarbeiters, der Haftung dann zu entgehen, wenn dieser „nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“.

3.2.2.4.5 Speziell: § 7 StVG und § 18 StVG

Neben diesen – grundsätzlich für alle automatisierten Systeme relevanten – Haftungsnormen sind für spezifische automatisierte Systeme weiterhin auch Haftungsnormen aus diversen Spezialgesetzen zu beachten.

Im Rahmen von Straßenfahrzeugen ist dabei zunächst § 7 Abs. 1 StVG sowie § 18 Abs. 1 StVG relevant: Gem. § 7 Abs. 1 StVG haftet der Fahrzeughalter verschuldensunabhängig (Gefährdungshaftung), wenn bei dem Betrieb seines Kraftfahrzeugs ein Mensch getötet, der Körper oder die Gesundheit eines Menschen verletzt oder eine Sache beschädigt wird. Neben dieser Halterhaftung kann nach § 18 Abs. 1 StVG auch der Fahrzeugführer zur Haftung gezogen werden mit dem Unterschied, dass hierbei ein Verschulden dessen (Vorsatz oder Fahrlässigkeit) vorliegen muss. Das Vorliegen dieses Verschuldens wird dabei zunächst aber vermutet und kann von dem Fahrzeugführer lediglich durch Exkulpation, also durch das Erbringen eines Gegenbeweises, ausgeräumt werden.

Mit zunehmenden Automatisierungsgrad des Kfz stellen sich hinsichtlich dieser Haftungsnormen zwei Grundsatzfragen: zum einen ist hierbei fraglich, wie künftig eine adäquate Haftungsteilung zwischen dem Fahrzeughalter und dem Produzenten vorzunehmen ist, wenn bei höher automatisierten Systemen die Ursache eines Unfalls meist in der Fahrzeugfirmware und daher in der Sphäre des Entwicklers liegt. Zum anderen ist fraglich, ob auch bei höher automatisierten Systemen (insbesondere ab der Stufe der Vollautomatisierung, bei der eine eigene Steuerung des Fahrers stark zurücktritt) überhaupt noch ein „Fahrzeugführer“ im klassischen Sinne vorhanden ist. Denn wird

dem Fahrer durch eine fortgeschrittene Fahrzeugautomatisierung erlaubt, sich während der Fahrt auch mit anderen Dingen zu beschäftigen, sind zu diesem Zeitpunkt ggf. alle Insassen des Kfz nur noch als Passagiere anzusehen (u.U. aber mit der Möglichkeit der manuellen Steuerungsübernahme oder des Einlenkens).[38]

3.2.2.4.6 Speziell: § 33 LuftVG

Als spezifische Haftungsnorm bei dem Einsatz automatisierter Industrie- oder Dienstleistungsdrohnen kommt weiterhin § 33 Abs. 1 LuftVG in Betracht. Hiernach haftet der Halter des Luftfahrzeugs, wenn bei dem Betrieb durch einen Unfall jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt wird.[39] Zu Regulierung etwaiger Schäden durch die Nutzung von Drohnen ist der Abschluss einer spezifischen Haftpflichtversicherung Pflicht. Die normale Privathaftpflichtversicherung deckt durch Drohnen verursachte Schäden in der Regel nicht ab.

Auch hierbei stellt sich im Laufe der Fortentwicklung des Automatisierungsgrades bei Industrie- und Dienstleistungsdrohnen die Frage, wie eine adäquate Haftungsteilung zwischen dem Luftfahrzeughalter und dem Produzenten des Luftfahrzeugs realisiert werden kann, da mit zunehmenden Automatisierungsgrad die Ursache eines Unfalls auch hierbei meist Folge eines Soft- oder Hardwarefehlers und daher eher der Sphäre des Entwicklers und Herstellers zuzuschreiben sein wird.

---

[38] Vgl. zu den Rechtsfragen des automatisierten Fahrens auch vbw, Position - Zukunft automatisiertes Fahren: Rechtliche Hürden beseitigen, S. 17 ff.

[39] Hinsichtlich der Haftung bei der Beförderung von Fluggästen existieren dagegen spezifische Haftungsnormen, vgl. etwa §§ 44 ff. LuftVG. Diese sollen im Rahmen dieses Gutachtens aber außer Betracht gelassen werden.

4 Ausblick

Automatisierte Systeme werden zukünftig unser Leben mitbestimmen. Nicht nur unsere Häuser und Wohnungen werden intelligent und vernetzt. Auch unsere Autos werden untereinander kommunizieren, unsere Bestellungen werden minutenschnell per Drohne geliefert und sogar unsere Kleidung wird „smart“.

Diese umfassende Automatisierung sowie Vernetzung und damit „Smartifizierung“ unseres Alltags bringt neuartige Rechtsfragen mit sich, die mehrheitlich zwar auch durch das geltende Recht beantwortet werden können. Dennoch fehlen hier auch stellenweise automatisierungsspezifische Regelungen. Dies betrifft, wie gezeigt wurde, insbesondere etwa das IT-Sicherheitsrecht, das bislang lediglich als „Flickenteppich“ unterschiedlichster und kaum überschaubarer Normen existiert.

Das deutsche Haftungsrecht hält dagegen eine Vielzahl an haftungsbegründenden Vorschriften bereit, die auch für die Anwendung in automatisierten Systemen als ausreichend gelten müssen. Dies ist jedenfalls so lange der Fall, wie auch künstlich intelligente und selbstlernende Systeme sich nur im Rahmen der vorgegebenen Programmierung bewegen können und letztendlich auf die Vorgaben eines Menschen zurückzuführen sind, der oder dessen Organisation letztendlich haftbar gemacht werden kann. Probleme bestehen hier aber in der Vermeidung von Haftungslücken und Haftungsverschiebungen, wenn sich der Kausalverlauf eines Unfalls mit einem Roboter nicht rechtssicher nachvollziehen und beweisen lässt. Hier müssen ausgefeilte technische Lösungen ansetzen, die die Beweisbarkeit von Prozessen in automatisierten Systemen gewährleisten.

Die Automatisierung unseres Alltags sowie unserer Industrie und Wirtschaft wird daher nicht nur eine gesetzgeberische Herausforderung sein, vielmehr muss dieser auch durch eine rechtskonforme und innovative Technikgestaltung begegnet werden.

Ansprechpartner

Christine Völzow
Büroleiterin des Präsidenten und des Hauptgeschäftsführers

Telefon 089-551 78-104
Telefax 089-551 78-106
christine.voelzow@vbw-bayern.de

Impressum

Alle Angaben dieser Publikation beziehen sich grundsätzlich sowohl auf die weibliche als auch auf die männliche Form. Zur besseren Lesbarkeit wurde meist auf die zusätzliche Bezeichnung in weiblicher Form verzichtet.

Herausgeber:

vbw
Vereinigung der Bayerischen Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de

Verfasser:

Prof. Dr. Dirk Heckmann
Lehrstuhl für Öffentliches Recht, Sicherheitsrecht u. Internetrecht
Universität Passau

Telefon 0851-509 22-90
heckmann@mein-jura.de

Dipl.-Jur. Alexander Schmid
Lehrstuhl für Öffentliches Recht, Sicherheitsrecht u. Internetrecht
Universität Passau

mail@schmid-recht.de